Titre: Title:	Routage proactif alterné basé sur la qualité de service UMTS
Auteur: Author:	Gerry Dorvius
Date:	2003
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Dorvius, G. (2003). Routage proactif alterné basé sur la qualité de service UMTS [Mémoire de maîtrise, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/7244/

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

ROUTAGE PROACTIF ALTERNÉ BASÉ SUR LA QUALITÉ DE SERVICE UMTS

GERRY DORVIUS
DÉPARTEMENT DE GÉNIE INFORMATIQUE
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION
DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES
(GÉNIE INFORMATIQUE)
AOÛT 2003

Your file Votre référence
ISBN: 0-612-89197-6
Our file Notre référence
ISBN: 0-612-89197-6

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

ROUTAGE PROACTIF ALTERNÉ BASÉ SUR LA QUALITÉ DE SERVICE UMTS

Présenté par : DORVIUS Gerry

En vue de l'obtention du diplôme de : Maîtrise ès sciences appliquées

A été dûment accepté par le jury d'examen composé de :

M. GAGNON Michel, Ph.D., Président

M. PIERRE Samuel, Ph.D., Directeur

M. QUINTERO Alejandro, Ph.D., Membre

REMERCIEMENTS

Je tiens à remercier chaleureusement mon directeur de recherche, monsieur Samuel Pierre, pour son soutien et son encadrement tout au long de mon travail de recherche.

Je tiens également à remercier monsieur Yves Lemieux de Ericsson Recherche Canada pour avoir supervisé mon stage dans le cadre de la Chaire CRSNG-ERICSSON en Systèmes Réseautiques Mobiles de Prochaines Générations.

Mes remerciements vont aussi aux membres du LARIM et mes collègues de stage pour l'ambiance de travail amicale.

Finalement, je tiens à exprimer ma profonde gratitude aux membres de ma famille et mes amis qui m'ont apporté beaucoup de support au cours de ce travail.

RÉSUMÉ

La survivabilité des réseaux mobiles est l'un des aspects les plus importants dans la gestion de fautes des réseaux afin d'assurer une haute disponibilité et une protection aux pannes. Étant donné que les topologies de ces réseaux varient continuellement dans le temps, la découverte rapide d'un chemin alterné après une panne de nœud ou de lien devient critique. Cela implique que les LSR supportent des mécanismes de détection et de notification de pannes, et que les protocoles de signalisation puissent supporter la configuration de chemins primaires et alternés. Les LSR sont des routeurs qui ont la capacité de router des paquets en se basant sur la technologie MPLS. Au cours des dernières années, plusieurs mécanismes ont été développés pour garantir une réponse rapide aux pannes de réseaux. Parmi ces solutions, on retrouve la *Protection par commutation* (*Protection Switching*) et le *Reroutage Rapide* (*Fast Reroute*).

La *Protection par commutation* est une méthode par laquelle les données sont commutées d'un chemin primaire en panne à un chemin secondaire préalablement défini pour assurer sa protection. Le *Reroutage Rapide* est une technique permettant d'établir des chemins de protection autour d'un lien, un nœud ou une portion de LSP jugé critique. Lors d'une panne sur l'élément protégé, les données sont transférées sur le chemin de réservé pré-établi.

Ces deux mécanismes offrent un temps de complétion rapide, mais ils reposent sur des LSP réservés et pré-établis, ce qui entraîne une mauvaise optimisation des ressources. De plus, ces mécanismes ne tiennent pas compte des différentes classes de trafic, comme le trafic UMTS, lorsqu'ils assurent la protection.

L'objectif de notre recherche est de présenter un algorithme de reroutage capable d'optimiser l'utilisation des ressources du réseau, et qui tient compte des requis de qualité de service d'un trafic UMTS. L'algorithme sera appliqué sur un réseau dorsal IP/MPLS d'un réseau mobile sans-fil supportant des trafics UMTS en accès. Nous avons considéré un réseau quasi-statique.

Nous avons proposé un algorithme de survivabilité qui combine les avantages de la *Protection par commutation* et du reroutage alterné. Ce nouvel algorithme est le premier du genre à prendre en considération les requis de qualité de service du trafic lors du calcul de chemins alterné. Afin d'assurer la validité de notre approche, nous avons d'abord posé certaines hypothèses simplificatrices qui déterminent le domaine d'utilisation. Ensuite, nous avons énoncé les principales actions de l'algorithme dans des cas bien précis. Nous avons terminé le travail en effectuant une analyse de performances à l'aide de simulations, qui nous a permis de tester différents cas.

Le modèle de simulation développé, pour évaluer et valider les performances de l'algorithme de routage alterné proactive proposé, utilise le langage C sur le logiciel OPNET. Les résultats de simulation montrent que l'algorithme est stable et offre de bonnes performances pour le temps de reroutage et le délai de transmission de bout en bout. C'est donc une bonne solution de compromis aux problèmes de temps de réponse et d'optimisation de ressources posés par les mécanismes traditionnels. De plus, l'algorithme offre l'avantage d'être facile à implémenter, de limiter les messages de mises à jour de table de routage, et d'optimiser les ressources du réseau.

ABSTRACT

The survivability of mobile network is one of the most important aspects in fault management in order to ensure high network reliability and fault protection. Given that network topologies are never stable over time, rapid response to link or node failures and/or congestion by means of rerouting is critical. This requires that the LSR support failure detection and notification, and that LSP signaling support the configuration of working and protection paths. An LSR is a router capable of routing data packets based on the MPLS technology. Several mechanisms have been developed in the past years to guarantee rapid responses to network failures and congestion. Some of theses solutions are *Protection Switching* and *Fast-Reroute*.

Protection Switching is a method in which data is switched from a failed LSP to a backup LSP at the repair point (usually the ingress LSR). *Fast-reroute* is a process where MPLS data can be directed around a link or node failure without the need to perform any signaling at the time the failure is detected.

Both of these mechanisms offer fast response time, but rely on pre-established LSP, which results in bad resources optimization. Furthermore, they don't take into account the different classes of traffic in a network, such as UMTS, when offering protection.

The objective of our research is to present a rerouting algorithm that optimizes network resource utilization and that takes into account the QoS requirements of UMTS traffic classes. The algorithm will be applied to an IP/MPLS backbone of a mobile network that supports access to UMTS and W-LAN.

We are proposing a survivability algorithm that combines the advantages of *Protection Switching* and *Fast-Reroute*. This new algorithm is the first to take into account the UMTS quality of services requirements when computing an alternate path for protection purposes. In order to validate our approach, we have made some assumptions that allow us to better define the application domain of the mechanism. Then, we

described the action performed by the algorithm in specific cases. We have concluded our work by evaluating the performance of our approach by simulations.

A simulation model has been developed to evaluate and validate the performance of our proactive alternate routing algorithm. It has been written in C using the OPNET Modeler simulation software. The simulations that have been conducted show that the algorithm is stable and offers good rerouting time and delay. The algorithm can be considered as a good solution to the issues raise by completion time and resources optimization in the context of survivability. Moreover, it has several advantages such as simple implementation, limited exchange of routing information between network nodes, and optimization of network resources.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTES DES TABLEAUX

LISTE DES SIGLES ET ABRÉVIATIONS

A	Availability ratio
ATM	Asynchronous Transfer Mode
BG	Border Gateway
CR-LDP	Constrained Routing – Label Distribution Protocol
CSPF	Constrained Shortest Path First
DS	Digital Signal or Data Service level
DS0	64 Kb/s transmission data rate
DS1	1.544 Mb/s transmission data rate
DS1C	3.15 Mb/s transmission data rate
DS2	6.31 Mb/s transmission data rate
DS3	44.736 Mb/s transmission data rate
DS4	274.1 Mb/s transmission data rate
DiffServ	Differentiated Services
EF	Expedited Forwarding
ERO	Explicit Route Object
FEC	Forwarding Equivalence Class
FIS	Failure Indication Signal
FRS	Failure Recovery Signal
HQ	High Quality
IETF	Internet Engineering Task Force
IntServ	Integrated Services
IOS	Internetwork Operating System
IP	Internet Protocol
IS-IS	Intermediate System-to-Intermediate System
LAN	Local Area Network
LDP	Label Distribution Protocol
LER	Label Edge Router

LM	Liveness Message
LQ	Low Quality
LSP	Label Switched Path
LSR	Label Switch Router
ME	Mobile Equipment
MP	Merge Point
MPLS	Multi-Protocol Label Switching
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
NHOP	Next Hop
NNHOP	Next Next Hop
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PHB	Per Hop Behavior
PLR	Point of Local Repair
PML	Path Merge LSR
PSL	Path Switch LSR
PSTN	Public Switched Telephone Network
PAR-UMTS	Proactive Alternate Routing for UMTS
QoS	Quality of Service
RC	Resilience Class
RD-QoS	Resiliency Differentiated Quality of Service
RIP	Routing Information Protocol
RNIS	Réseau Numérique à Intégration de Services
RRO	Record Route Object
RSVP-TE	Resource Reservation Protocol Traffic Engineering
SONET	Synchronous Optical Network
TCP	Transmission Control Protocol
TE	Traffic Engineering

TOS	Type of Service
TLV	Type Length Value
U	Unavailability ratio
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network
WLAN	Wireless LAN

CHAPITRE I
INTRODUCTION

L'avènement de l'Internet et les ambitions de convergence des trafics de voix, de donnée, et de vidéo sur un réseau commun entraîne plusieurs défis de recherche pour la communauté scientifique. Parmi ces défis, on retrouve la nécessité d'élaborer des mécanismes permettant d'assurer la fiabilité des réseaux de communications. Cette fiabilité peut être vue sous deux aspects : la disponibilité du réseau et la survivabilité. La disponibilité réfère à la capacité du réseau à exécuter ses fonctions à n'importe quel instant donné, tandis que la survivabilité désigne la capacité du réseau à effectuer ses fonctions même en présence de panne. Pour assurer cette survivabilité, plusieurs mécanismes ont été élaborés et déployés au cours des années. Étant donné que la technologie MPLS offre de nombreux avantages permettant d'assurer la convergence sur des réseaux dorsaux IP, il devient alors pertinent de s'interroger sur les différentes manières de rendre les réseaux MPLS plus survivables, ce qui constitue l'objet de ce mémoire. Dans ce chapitre d'introduction, nous allons d'abord définir les concepts de base des réseaux MPLS et des mécanismes de survivabilité. Ensuite, nous présenterons la problématique de recherche qui fait l'objet de ce mémoire, suivi d'un énoncé des objectifs visés, de l'esquisse méthodologique, et des principaux résultats attendus de cette recherche. Enfin, nous esquisserons le plan du mémoire.

1.1 Définitions et concepts de base

L'acronyme MPLS réfère à *MultiProtocol Label Switching*. C'est une technologie qui peut être implémentée indépendamment des protocoles utilisés sur les couches 2 et 3 du modèle OSI. Dans le cas de l'Internet, MPLS permet d'ajouter certaines fonctionnalités aux réseaux IP traditionnels :

- l'acheminement rapide des données de l'usager ;

- l'ingénierie du trafic (*Traffic Engineering- TE*), qui permet une optimisation des ressources du réseau par une répartition intelligente du trafic ;
- le traitement du trafic avec des contraintes de qualité de service (QoS) spécifiques, et le routage avec contraintes ;
- l'établissement de réseaux privés virtuels (VPN).

Un chemin est constitué de l'ensemble des nœuds et des liens que doit parcourir le trafic d'une source à une destination. On réfère aussi à un chemin par le terme chemin. Dans ce mémoire, on considérera que les chemins entre un nœud source et destination sont disjoints.

Les principales composantes d'un réseau MPLS sont les LSR, les LSP, les étiquettes (*Label*), les nœuds *Ingress* et *Egress*, et les FEC; elles sont illustrées à la Figure 1.1. Les LSR (*Label Switched Router*) sont des routeurs munis d'un logiciel d'exploitation (IOS ou *Internetwork Operating System*) offrant des fonctionnalités MPLS.

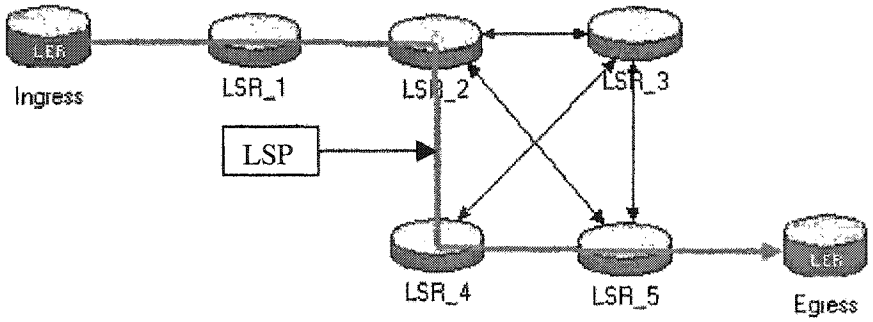

Figure 1.1 Composante d'un réseau MPLS

Un LSP (*Label Switched Path*) représente le chemin qu'un ensemble de paquets doit suivre entre une source et une destination à l'intérieur d'un domaine MPLS. Le domaine MPLS est composé de l'ensemble des LSP et LSR situés entre un *Ingress* et un *Egress*. L'*Ingress* est un LSR qui reçoit des paquets IP provenant d'un domaine IP, qu'il encapsule et envoie sur un LSP du domaine MPLS. Le routeur *Egress* reçoit les paquets

provenant d'un LSP et les envoie sur un domaine IP. À l'intérieur du domaine MPLS, le routage s'effectue à l'aide d'étiquettes, contrairement au routage IP qui est basé sur l'adresse de destination (réseau) des paquets. L'avantage d'utiliser des étiquettes est qu'ils permettent d'acheminer les paquets sur la base de leurs adresses source, destination ou sur la base des contraintes liées à la qualité de service. L'ensemble de paquets qui doivent recevoir un traitement identique entre la source et la destination correspond à un FEC (*Forwarding Equivalence Class*). On peut aussi préétablir des chemins pour certains types de trafic.

Lorsque le LSR reçoit un paquet, il encapsule le paquet en lui ajoutant une étiquette MPLS. C'est sur la base de l'étiquette incluse dans l'en-tête de chaque paquet que le LSR va router le paquet et, selon ce qui est indiqué dans sa table de routage, il échangera la valeur des étiquettes (*Label swapping*), il ajoutera une étiquette (*Push*) ou il retirera l'étiquette (*Pull*).

Lorsqu'on effectue la protection de réseaux MPLS contre des pannes, le LSP qui sert à transmettre le trafic est désigné comme un LSP ou chemin primaire. Le LSP qui sert à protéger le LSP primaire est appelé un LSP de réserve ou LSP secondaire.

Les classes de trafic que l'on va tenter de protéger dans le cadre du mémoire sont des trafics UMTS (*Universal Mobile Telecommunications System*). Quatre classes de trafic sont définies dans UMTS : la classe *Conversational* qui comprend la voix et la vidéo-conférence; la classe *Streaming* comprenant la vidéo sur demande; la classe *Interactive* qui comprend le trafic HTTP, TELNET, FTP; et finalement la classe *Background* dont les messages électroniques font partie.

1.2 Éléments de la problématique

Un des éléments marquants des dernières années a été l'émergence de l'Internet à l'échelle de la planète. Internet permet à n'importe quel usager à travers le monde de communiquer avec d'autres individus à des distances éloignées et ce, à des prix abordables. Avec l'Internet, on peut s'échanger des messages et des documents, et télécharger de l'information à distance. Cependant, dus aux contraintes du protocole IP,

qui est le protocole de niveau 3 (Modèle OSI) utilisé pour le routage dans Internet, la communication sur le WEB était jusqu'à ce jour limitée à la transmission de données.

Pour bien comprendre les limites de IP, il faut d'abord comprendre les caractéristiques des deux grandes catégories d'information. En télécommunications, on fait la distinction entre la transmission de la voix et la transmission de données. La transmission de voix génère un trafic de voix résultant de la communication entre deux individus par téléphone. La voix étant très sensible aux délais, elle requiert une connexion dédiée où le chemin ou circuit est prédéterminé et la disponibilité des ressources est garantie. Le mode de transmission de la voix est la commutation de circuits. Dans la commutation de circuits, lorsqu'un usager veut communiquer avec un autre, le réseau établit un chemin dédié entre les deux entités communicantes. Pour établir ces circuits, on utilise des circuits point-à-point (T1 ou T3), RNIS, ATM ou encore le réseau PSTN.

L'autre catégorie de transmission est la transmission de données. Les informations transmises sont autres que de la voix. Elles sont subdivisées en paquets. Étant donné que les contraintes de délai et de qualité de service sont moins restrictives pour le trafic de données, le chemin entre la source et la destination n'est pas réservé avant la connexion, comme c'est le cas avec la voix. Les paquets sont routés à l'aide du protocole IP qui utilise des protocoles de routage tel RIP (*Routing Information Protocol*) ou OSPF (*Open Shortest Path First*) pour connaître le chemin le plus court et avoir une vue globale du réseau. Une des faiblesses de ce type de communication est que les données sont toujours transmises sur le plus court chemin, ce qui peut donner lieu à de la congestion, des délais de transmission, et la perte de paquets. C'est un mode de transmission qui convient aux trafics de données, mais qui est inacceptable pour la voix. De plus, étant donné que le trafic emprunte le plus court chemin, les ressources sur les chemins plus longs sont souvent sous-utilisées. C'est cette catégorie de transmission qui est présentement supportée par Internet.

Depuis quelques années, le mot clé en communication est *convergence*. La *convergence* implique de pouvoir transmettre sur un même réseau divers types de trafics

(voix, données, et multimédia). Cette convergence implique de pouvoir offrir à chaque type de trafic la qualité de service nécessaire.

Un élément clé qui permettra d'effectuer cette convergence sur le WEB est l'arrivée du protocole MPLS. C'est un protocole qui permet de combiner les avantages de la communication IP traditionnelle (commutation de paquets) avec les avantages de la communication de voix (commutation de circuits). MPLS est indépendant du protocole utilisé aux couches liaison (2) et réseau (3) du modèle OSI. De plus, il permet de faire de l'ingénierie de trafic (*Traffic Engineering*), qui consiste essentiellement à placer le trafic là où la largeur de bande est disponible et à optimiser les ressources du réseau. Il permet d'établir des chemins dédiés entre deux points, ce qui diminue la congestion. Il dispose en plus de mécanismes tels *Integrated Service (IntServ)* et *Differentiated Service (DiffServ)* qui permettent de réserver des ressources et d'offrir un traitement adéquat (QoS spécifique) aux différents types de trafic.

La survivabilité et la protection aux fautes est l'un des aspects les plus importants dans la gestion de réseaux MPLS. Étant donné que les topologies de réseaux ne restent pas stables dans le temps, un temps de réponse rapide suite à une panne de nœud ou de lien s'avère critique, surtout pour le trafic de voix et de vidéo-conférence. Cela implique que les LSR doivent supporter la détection de fautes, la notification de fautes et les mécanismes de protection. Cela implique également que la signalisation des LSP supporte la configuration de chemins primaires et de réserve. Plusieurs mécanismes ont été développés au cours des dernières années afin de garantir une réponse rapide aux pannes de réseaux et à la congestion. Parmi ces solutions, on retrouve la *Protection par commutation* (*Protection Switching*) et le *Reroutage rapide*(*Fast-Reroute*).

La *Protection par commutation* est une méthode de protection selon laquelle les données sont transférées sur un chemin de réserve en cas de panne sur le chemin primaire. C'est un mécanisme de protection globale, qui assure la protection de l'*Ingress* jusqu'à l'*Egress*. Le *Reroutage rapide* est un mécanisme qui permet de rediriger le trafic autour du point de défaillance en cas de panne. C'est une protection locale, puisque les chemins de réserve sont établis autour des points susceptibles de subir une défaillance.

Les deux mécanismes offrent des temps de restauration faibles, mais ils se basent sur des chemins préétablis, ce qui résulte en une sous-utilisation des ressources du réseau. De plus, ces mécanismes ne tiennent pas compte des différentes exigences de qualité de service liées aux divers types de trafics UMTS. Ce mémoire s'inscrit donc dans le cadre de travaux de recherche visant à développer un mécanisme qui assurera un temps de réponse rapide pour chaque type de trafic et qui optimisera les ressources du réseau.

1.3 Objectifs de recherche

L'objectif principal de ce mémoire est de concevoir un algorithme de routage permettant de trouver des chemins alternés qui respectent, dans la mesure du possible, les contraintes de qualité de service liées aux types de trafic UMTS, tout en offrant un temps de complétion comparable à celui offert sur les réseaux SONET pour les trafics de voix et de vidéo-conférence. Plus spécifiquement, ce mémoire vise à :

- analyser les algorithmes de routage existants en vue de déceler leurs faiblesses eut égard à leur incapacité de satisfaire les contraintes de qualité de service ;
- concevoir et implémenter un algorithme proactif de routage alterné qui sera basé sur les contraintes de qualité de service de chaque classe de trafic UMTS et sur les ressources disponibles sur le réseau ;
- évaluer l'impact de cet algorithme sur la qualité de service associée à chacune des quatre classes de trafic UMTS ;
- comparer cet algorithme avec le mécanisme de *Fast-Reroute/Protection Switching* implémenté dans OPNET, en tant que mécanisme garantissant le meilleur temps de réponse suite à une panne.

Les chemins alternés calculés par cet algorithme seront sauvegardés dans la mémoire *Cache* des LSR et seront mis à jour à chaque changement de topologie.

1.4 Esquisse méthodologique

Afin de réaliser notre algorithme de routage alterné, nous allons suivre la méthodologie suivante.

Premièrement, nous allons analyser les algorithmes existants. Deuxièmement, on proposera une solution en définissant le contexte d'utilisation de l'algorithme et en établissant des hypothèses de départ permettant de simplifier l'implémentation et l'analyse. Ces hypothèses porteront sur :

- le type de réseau et la topologie, i.e. une dorsale IP utilisant MPLS, le nombre de nœuds/routeurs, le type de liaisons, le nombre de chemins disjoints, les largeurs de bande disponibles ;
- les paramètres de performance, i.e. le taux d'utilisation des liens, le taux d'erreur, et le délai acceptable pour chaque classe de service ;
- le protocole utilisé au niveau de la couche réseau (IP dans ce cas), le protocole de routage (RIP, OSPF, IS-IS, etc.), le protocole de signalisation des LSP (RSVP, CR-LDP, LDP) ;
- les caractéristiques du trafic à protéger; dans notre cas, ce sera un trafic UMTS provenant d'un réseau d'accès connecté à la dorsale.

Deuxièmement, on déterminera les cas de bris typiques, bris de liens et de nœuds, ainsi que les actions à suivre lors de ses bris. Des scénarios devront être créés de manière à couvrir tous les cas possibles. Une fois les scénarios créés, on définira les grandes lignes de l'algorithme, puis le plan de test.

La troisième étape sera de construire un prototype sur OPNET qui est représentatif des hypothèses établies à la deuxième étape. Nous implémenterons l'algorithme et nous élaborerons un plan de test avec les bris à simuler, les paramètres à mesurer et les résultats attendus.

Il sera aussi intéressant de comparer les résultats du nouvel algorithme avec une méthode de référence qui, dans notre cas, sera le *Fast-Reroute/Protection Switching* qui a déjà été implémenté dans OPNET.

1.5 Plan du mémoire

Le mémoire comporte quatre autres chapitres en plus de ce chapitre introductif. Le second chapitre est une synthèse des différents mécanismes de survivabilité qui sont présentement utilisés pour assurer la protection de réseaux vis à vis des fautes. Le troisième chapitre présente un algorithme de routage pro-actif : l'algorithme de routage alterné proactif basé sur la qualité de service UMTS (*Proactive Alternate Routing for UMTS*); il présente ensuite la modélisation, l'implémentation et la mise en œuvre. Le quatrième chapitre expose les expériences et les mesures effectuées pour l'évaluation de performance, analyse et discute les résultats en les comparant à la méthode de *Fast-Reroute/Protection Switching*. Le cinquième et dernier chapitre fait une synthèse des résultats obtenus, discute des limitations des travaux et indique des repères de recherche future.

CHAPITRE 2
MÉCANISMES DE SURVIVABILITÉ

L'émergence du protocole MPLS pour le routage de trafic sur Internet a eu un grand impact sur l'ingénierie du trafic (*Traffic Engineering*). Les éléments qui constituent l'architecture MPLS sont : les LSP (*Label Switched Path*), la découverte efficace de chemin sur le réseau, l'assignation du trafic à des LSP et une réponse rapide aux changements de topologie du réseau. Étant donné que les topologies de réseau ne restent pas stables, un reroutage rapide suite à un bris de lien/nœud ou à une forte congestion devient critique. Plusieurs mécanismes ont été développés pour garantir une réponse rapide suite à une panne ou de la congestion. Parmi ces solutions, on retrouve la *Protection par commutation* (*Protection Switching*) et le *Reroutage rapide* (*Fast Reroute*). Dans ce chapitre, nous présenterons différentes méthodes qui sont actuellement utilisées pour permettre la protection des réseaux IP/MPLS et assurer la survivabilité de ces réseaux. On débutera en donnant une brève description des mécanismes de gestion de fautes dans MPLS. Ensuite, on décrira en détail les deux principaux mécanismes actuellement utilisés : la *Protection par commutation* (*Protection Switching*) et le *Reroutage rapide* (*Fast Reroute*). On terminera en décrivant le modèle RD-QoS, qui est une proposition intégrant les différents mécanismes de restauration afin d'assurer une protection basée sur les classes de services.

2.1 Architecture de protection dans MPLS

Les éléments suivants sont disponibles pour assurer la survivabilité des réseaux IP/MPLS (Ortega, 2001) :

- un mécanisme de sélection des chemins actifs/primaires et des chemins de réserve (*backup path*) ;
- un mécanisme pour la réservation des largeurs de bande pour les chemins actifs et de réserve ;

- un mécanisme pour la signalisation et l'établissement des LSP actifs et de réserve ;
- un mécanisme de détection de fautes et de pannes ;
- un mécanisme de notification pour informer les composants du réseau de la présence d'une panne ou d'une faute ;
- un mécanisme de commutation qui permet de transférer le trafic d'un LSP à un autre lors d'une panne ou d'une restauration.

La Figure 2.1 illustre un domaine de protection constitué de chemin principal (*LSP Working Path*), un chemin de réserve (*LSP Recovery Path*), ainsi que des PSL et PML. Les PSL (*Path Switch LSR*) et PML (*Path Merge LSR*) sont des LSR ayant des fonctions de protection et de restauration.

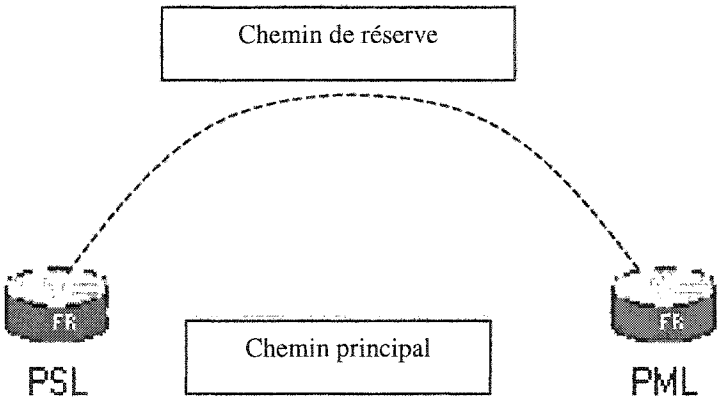

Figure 2.1 Domaine de protection MPLS

2.2 Concepts de base de MPLS

Pour mieux comprendre les mécanismes de gestion de fautes dans MPLS, il est nécessaire de connaître les concepts suivants (Ortega, 2001; Ping et al., 2002). Un chemin de réserve (*Backup Path*) est un LSP qui est chargé d'assurer la protection d'un autre LSP. Un chemin de réserve réfère à un LSP de détour (*detour LSP*) ou à un tunnel

de réserve (*Backup Tunnel*). Le LSP de détour (*Detour LSP*) est un LSP utilisé pour rerouter un trafic autour d'un lien/nœud en panne (*one-to-one backup*), alors que le tunnel de réserve (*Backup Tunnel*) est un LSP utilisé pour assurer la protection d'un ou de plusieurs LSP. Quant au tunnel d'évitement (*Bypass Tunnel*), il est utilisé pour protéger un ensemble de LSP empruntant un chemin commun. Un tunnel de contour de lien (*Next Hop (NHOP) Backup Tunnel*) contourne un lien du LSP protégé. Il est utilisé dans la protection de lien. La Figure 2.2 illustre un exemple de NHOP.

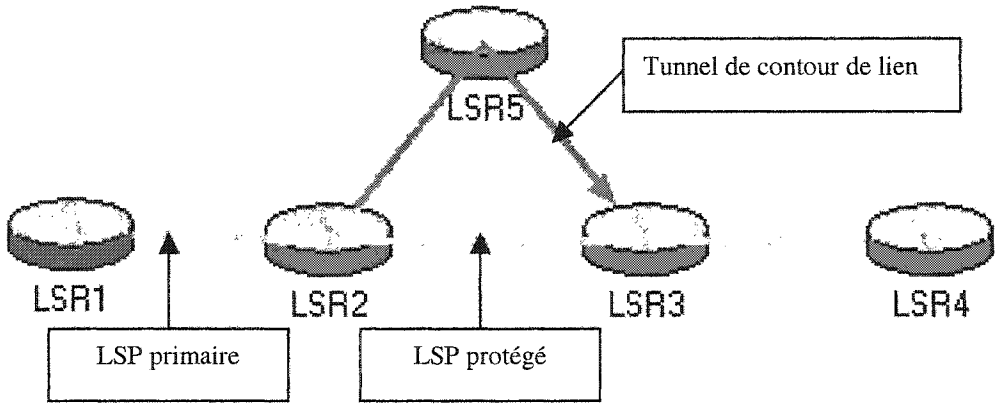

Figure 2.2 Tunnel de contour de lien (*Next-Hop Backup Tunnel*)

On retrouve aussi le tunnel de contour de lien et de nœud (*Next-Next-Hop (NNHOP) Backup Tunnel*), qui est un tunnel de réserve qui contourne un nœud du LSP protégé. Il est utilisé dans la protection de nœud, et protège autant contre le bris de lien qu'à celui de nœud. La Figure 2.3 illustre un exemple de NNHOP.

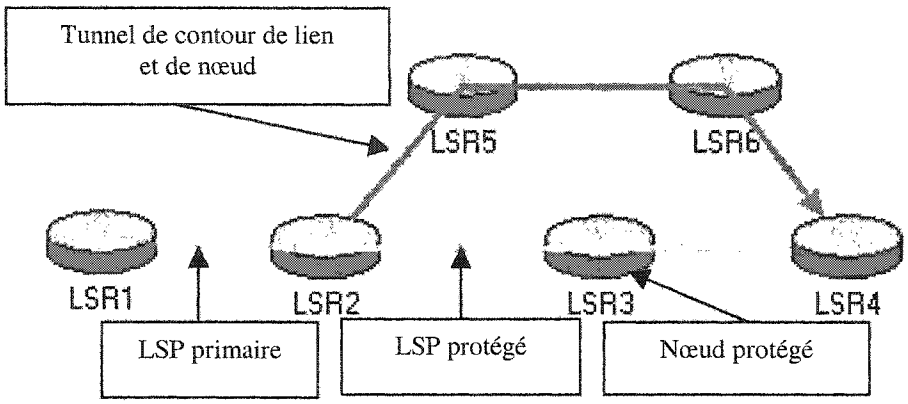

Figure 2.3 Tunnel de contour de lien et de nœud (*Tunnel Next-Next-Hop Backup*)

Un LSP (*Label Switched Path*) peut être défini comme un chemin ou un chemin MPLS. Un routeur capable de router de l'information avec le protocole MPLS est appelé LSR (*Label Switched Router*). Un point de rencontre (*Merge Point (MP)*) représente un LSR qui constitue le point de rencontre des tunnels de réserve et du chemin protégé après le point de fautes (*downstream*). Dans le cas du *one-to-one backup*, le MP peut aussi être un LSR où converge plusieurs détours; le MP est alors appelé un *Detour Merge Point*. Un MP peut aussi être un PLR. Le domaine de protection MPLS (*MPLS Protection Domain*) est l'ensemble des LSR et des LSP qui sont protégés. Un domaine de protection est dénoté par l'ensemble : (*working path, protection path*). On définit un point de protection locale (*Point of Local Repair (PLR)*) comme le point de départ (*head-end*) d'un tunnel de réserve ou d'un tunnel de détour. Un LSP qui possède un ou plusieurs tunnels de réserve est un LSP protégé (*Protected LSP*).

Le Signal d'indication de fautes (*Failure Indication Signal (FIS)*) est un signal qui indique qu'une panne a été détectée par un LSR voisin. Il consiste en une séquence de paquets transmis d'un LSR en aval vers un LSR en amont (*downstream LSR to an upstream LSR*). Ce message est retransmis par tous les LSR intermédiaires vers leurs voisins en amont, jusqu'à ce qu'il soit acheminé à un LSR capable d'initier la protection.

Le Signal de récupération (*Failure Recovery Signal (FRS)*) indique qu'une panne sur un chemin a été réparée. Il s'agit d'une séquence de paquets transmis d'un LSR en aval vers un LSR en amont. Ce message est retransmis par tous les LSR intermédiaires vers leurs voisins en amont, jusqu'à ce qu'il soit acheminé au LSR qui a initié la protection.

Un message de vivacité (*Liveness Message (LM)*) est échangé périodiquement entre deux LSR adjacents afin de surveiller un lien. Il assure l'intégrité du lien dans les deux directions, ainsi que la disponibilité du voisin. Il existe aussi deux types de pertes : la perte de signal et la perte de paquets. La perte de signal est un affaiblissement du signal qui résulte en l'incapacité d'une interface de le détecter, tandis que la perte de paquets est une altération de la couche MPLS qui est locale au LSR, et qui consiste en un abandon excessif de paquets sur une interface, abandon dû à une erreur d'étiquetage ou à des erreurs TTL.

2.3 Mécanismes de protection dans MPLS

Présentement, deux catégories de mécanismes sont utilisées pour assurer la protection des réseaux contre les défaillances : il s'agit des méthodes de protection globale (*Global Repair*) et des méthodes de protection locale (*Local Repair*). La technique le plus utilisée pour faire de la protection locale est la protection par commutation (*Protection Switching*) qui sera abordée dans la section 2.3.1, tandis que le reroutage rapide (*Fast-Reroute*) est la technique la plus utilisée pour faire de la protection locale, et sera abordé dans la section 2.3.2. Dans les deux cas, il faut établir des LSP de réserve qui serviront uniquement à transporter du trafic lors d'un bris. La différence entre les deux méthodes est que dans la protection globale, c'est le routeur de tête (*Ingress*) qui a la responsabilité de commuter le trafic du LSP actif au LSP de réserve, tandis que dans la protection locale, c'est le routeur qui détecte la défaillance qui à la responsabilité d'effectuer le transfert du trafic.

2.3.1 Protection globale – Protection par commutation

Dans la protection par commutation (*Protection Switching*), c'est le nœud *Ingress* qui a la responsabilité d'initier le mécanisme de protection lorsqu'il reçoit le signal d'indication de fautes (FIS). Cette méthode a l'avantage d'établir un seul LSP de réserve par LSP actif/groupe de LSP actifs, et seul le routeur de tête doit posséder l'intelligence nécessaire pour initier la protection.

Cependant, c'est une alternative coûteuse, car le message de signalisation d'erreur doit toujours être envoyé à la source, et le LSP de réserve ne doit servir qu'à la protection du LSP actif, donc il y a mauvaise utilisation des ressources.

La Figure 2.4 illustre une application de la protection globale. Dans cette figure, deux chemins sont établis : un chemin actif (i.e. LSR1-LSR3-LSR5-LSR6, en ligne pleine) et un chemin de réserve (LSR1-LSR2-LSR4-LSR6, en ligne pointillée).

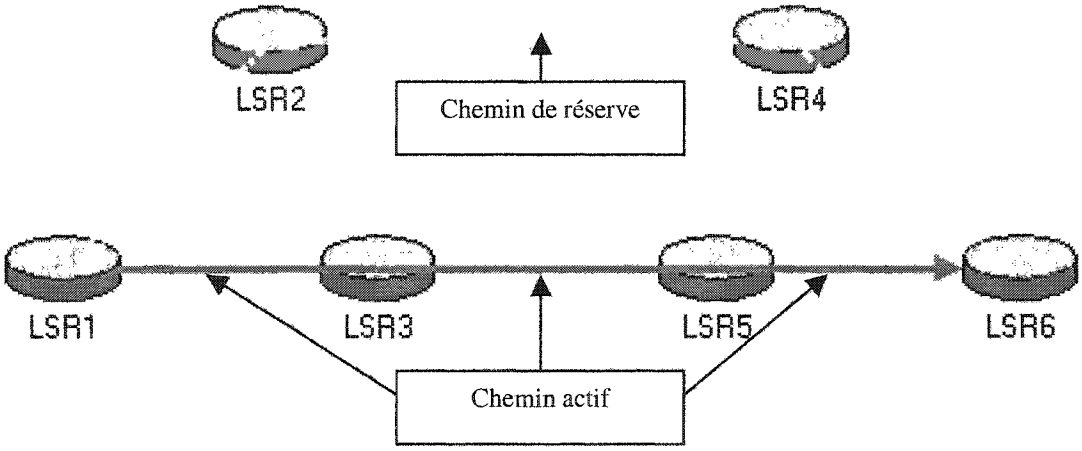

Figure 2.4 Protection Globale (Protection par commutation)

Dans la protection par commutation (*Protection Switching*), le chemin de réserve est généralement pré-établi. La Figure 2.5 montre deux chemins actifs qui sont protégés par un chemin de réserve. Lorsqu'une erreur est signalée au routeur de tête (*Ingress LER*), le trafic est commuté sur le chemin de réserve.

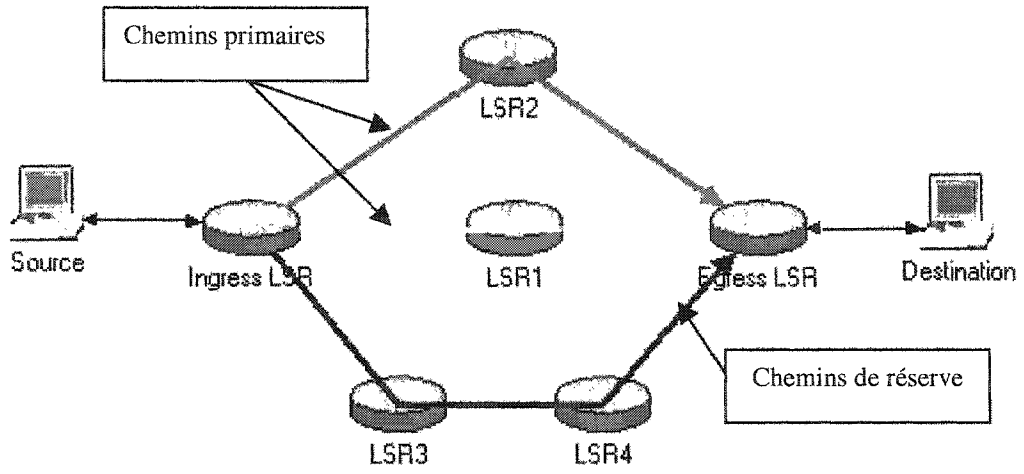

Figure 2.5 Protection par commutation (*Protection Switching*)

La protection par commutation offre plusieurs options lorsque le LSP de réserve est pré-établi :

- *Protection 1 + 1* : C'est la méthode de *Protection Switching* la plus rapide, puisque les données sont transmises simultanément sur les LSP actifs et de réserve. En cas de panne, le routeur de fin (*Egress LER*) lit les données provenant du LSP de réserve; lorsqu'il n'y pas de panne, il lit les données provenant du LSP actif ;
- *Protection 1 : 1* : Dans ce scénario, les données sont transmises uniquement sur le LSP actif. En cas de panne, le routeur de tête transfère les données sur le LSP de réserve. Étant donné que le LSP est réservé, on peut l'utiliser pour transmettre des données ayant de faibles contraintes au niveau de la qualité de service lorsqu'il n'y a pas de panne ;
- *Protection n : m* : Dans ce cas, *n* LSP actifs sont protégés par *m* LSP de réserve.

Notification d'erreurs

Lorsqu'une panne survient, elle doit être notifiée du point de détection au routeur de tête, de manière à ce que ce dernier puisse transférer le trafic du LSP actif au LSP de

réserve. Pour ce faire, les messages de notification *PathErr* dans RSVP-TE et *Withdraw* dans CR-LDP, peuvent être utilisé avec MPLS-TE. Le message de notification d'erreurs offre deux avantages au niveau de la performance :

- il est adressé au routeur de tête, donc il n'a pas à être traité par les routeurs intermédiaires ;
- le message est construit de telle sorte qu'il permet de signaler des pannes dans plusieurs LSP simultanément.

Vitesse de restauration

Le point critique avec la protection par commutation demeure la vitesse de restauration. Dépendamment du type de protection utilisé, la signalisation peut varier d'un simple message d'indication d'erreur à la signalisation complète d'un nouveau LSP. Plus il y a de signalisation, plus le temps de restauration augmentera; cependant, il est à noter que les systèmes qui requièrent beaucoup de signalisation optimisent mieux les ressources du réseau, car tous les nœuds ont une connaissance exacte de l'état du réseau.

Partage des ressources

Un autre désavantage de la protection par commutation est que les ressources du LSP de réserve sont pré-établies et ne peuvent donc être utilisées pour générer des revenus. Une solution consiste à partager les LSP de réserve entre plusieurs LSP actifs, tel qu'illustré à la Figure 2.6.

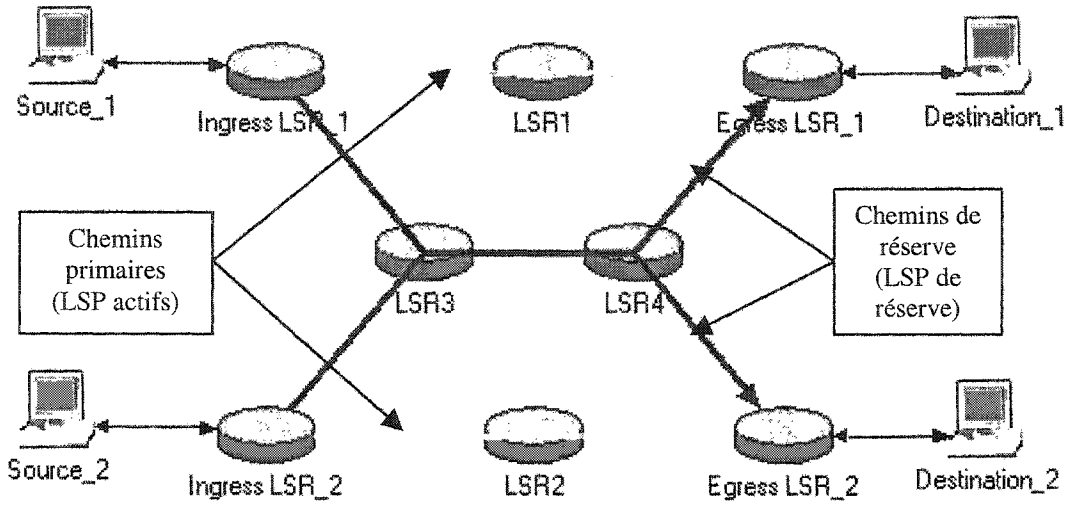

Figure 2.6 Partage de ressources de protection

2.3.2 Protection locale – *Reroutage rapide*

Dans le reroutage rapide (*Fast-Reroute*), il n'est plus nécessaire de remonter à la source pour initier la protection. La protection est initiée par le point de détection de la panne (PLR), ce qui diminue le temps de restauration. L'inconvénient de cette méthode est que tous les LSR qui doivent assurer la protection doivent être munis des fonctions d'un PSL, et un PML doit être défini. Cette méthode requiert aussi beaucoup d'entretien et la création de plusieurs LSP de réserve. La Figure 2.7 illustre un cas de protection locale. Le LSP actif est composé des routeurs LSR1-LSR3-LSR5-LSR6, et le LSP de réserve des routeurs LSR3-LSR4-LSR6. Lorsqu'une panne survient sur le lien formé par les routeurs LSR3-LSR5, le trafic est commuté sur le LSP de réserve.

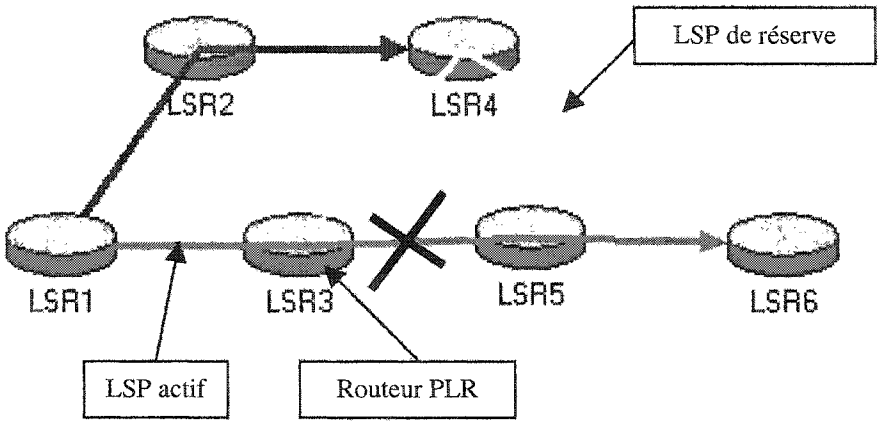

Figure 2.7 Protection locale

Dans une méthode de protection locale, les messages de signalisation sont routés par le protocole IP. Cela permet donc aux messages de signalisation d'utiliser de nouvelles routes pour atteindre leurs destinations.

Les trois méthodes de reroutage rapide (*Fast-Reroute*) les plus utilisées sont : la protection de lien, la protection de nœud et la protection de chemin.

Protection de lien

L'objectif de la protection de lien est de protéger un LSP d'une panne de lien. Dans la protection de lien, les chemins protégés et de protection sont disjoints. Quand le chemin protégé tombe en panne, le LSR de tête commute son trafic sur le LSP de protection. C'est une méthode de protection locale rapide, qui représente la forme la plus simple de reroutage rapide. Il peut être approprié dans des situations où certains éléments du réseau sont moins fiables que d'autres. La Figure 2.8 illustre un cas de protection de lien.

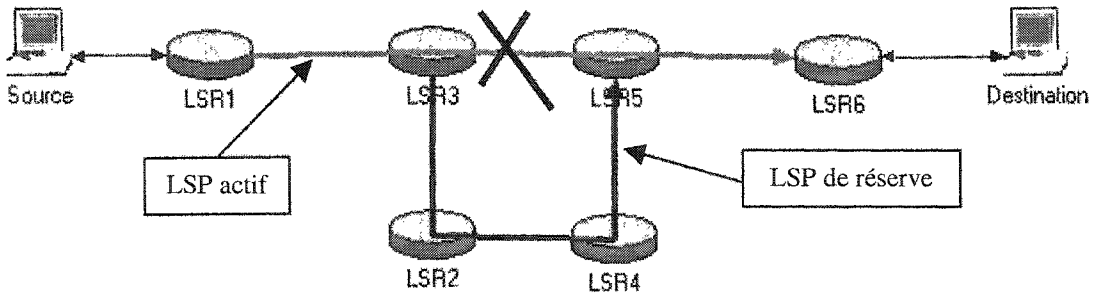

Figure 2.8 Reroutage rapide – Protection de lien

Lorsque le lien entre les LSR3 et LSR5 tombe en panne, le LSR3 transfère le trafic du LSP actif au LSP de réserve. Plusieurs contraintes doivent être prises en compte lorsqu'on établit des LSP de réserve. D'abord, la capacité du LSP de réserve doit être suffisante pour transporter le trafic du LSP protégé. Dans le cas où le LSP de réserve protégerait plusieurs LSP, sa capacité doit être égale à la somme des capacités des LSP protégés. Ensuite, il y a des contraintes sur les étiquettes à utiliser pour router le trafic. Lors de la panne, une étiquette qui représente le chemin de réserve est assignée au trafic, et par conséquent le routeur qui se situe de l'autre côté de la panne doit connaître cette étiquette de manière à acheminer le trafic comme s'il n'y avait pas eu de panne.

Finalement, l'implémentation de la protection de lien est complexe et c'est une méthode qui utilise beaucoup de ressources.

Protection de nœud

L'objectif de la protection de nœud est de protéger un LSP contre une panne de nœud. Les chemins protégés et de protection sont disjoints par rapport au nœud à protéger et aux liens associés à ce nœud. Quand le chemin protégé tombe en panne, le LSR de tête commute son trafic sur le LSP de protection. La Figure 2.9 montre un tunnel entre les LSR *A* et *C*, qui protège le LSR *B*. Lorsque le LSR *A* détecte la panne, il achemine le trafic vers le LSR *D*.

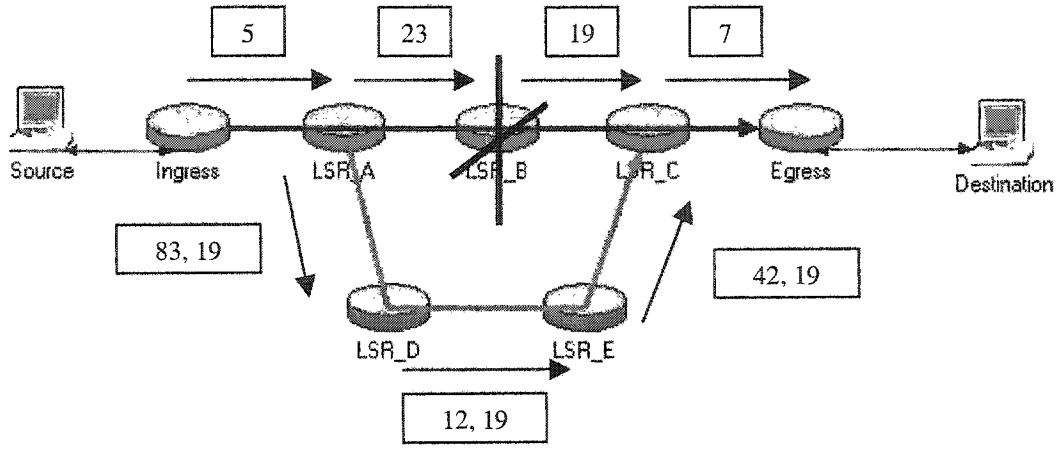

Figure 2.9 Reroutage rapide – Protection de lien

Une pile d'étiquettes est utilisée dans ce modèle, mais le problème est plus complexe car les routeurs LSR *A* et LSR *C* ne sont pas adjacents. Un paquet qui parcourt le lien de protection utilise une étiquette de haut niveau pour parcourir le LSP de protection et une étiquette de bas niveau (23) qui le relie au LSP original. Pour éviter toute confusion dans les étiquettes utilisées, on peut utiliser les récents ajouts apportés au protocole RSVP-TE en inscrivant les étiquettes utilisées dans le paramètre RRO (*Record Route Object*). Le RRO contient une liste de l'identité de chaque LSR et des étiquettes, et il est transmis en amont lors de l'établissement du LSP de manière à ce que chaque nœud sur le chemin ait une connaissance exacte des étiquettes utilisées sur chaque lien. Cela permet à chaque LSR de savoir quelle étiquette utiliser lorsqu'elle reroute le trafic après une panne. Ce processus peut être illustré par l'exemple de la Figure 2.9 (Farrel et Miller, 2001).

Dans la Figure 2.9, la progression des étiquettes sur le LSP originel à travers les LSR *A*, *B* et *C* est 5, 23, 19, 7. Le tunnel de réserve a les étiquettes 83, 12, 42. Si on utilisait la protection de lien, sans inscrire les étiquettes dans le RRO, les paquets envoyés du LSR *A* au LSR *D* auraient les étiquettes (83, 23), ce qui voudrait dire qu'une fois les paquets reçus par le LSR *C* l'étiquette serait 23 et le LSR ne saurait comment le traiter. Cependant, grâce à l'ajout dans le RRO, LSR *A* sait qu'il doit utiliser l'étiquette 19 lors

d'une panne pour que le LSR *C* puisse traiter le paquet convenablement. Une fois ce problème résolu, il faut traiter la question de l'espace d'étiquettes; l'approche la plus simple est d'utiliser un espace d'étiquettes global.

Protection de chemin

La protection de chemin permet de protéger un LSP en cas de panne à n'importe quel point du chemin. Le chemin de protection est complètement disjoint du chemin protégé. L'avantage de la protection de chemin est que le LSP de protection protège le chemin contre tous les types de pannes (lien, nœud ou les deux), excepté les pannes qui peuvent se produire à l'*Ingress* ou à l'*Egress*. De plus, étant donné que la sélection de chemin est point à point, la protection de chemin est plus efficace en terme d'utilisation de ressources que les protections de nœud ou de lien. Cependant, la commutation du trafic d'un chemin à un autre est, en général, plus lente avec la protection de chemin.

Un exemple de protection de chemin est illustré à la Figure 2.10. Si une panne survient au nœud *A*, les données sont transférées sur le chemin inverse (*Reverse Path*) vers le nœud *Ingress* pour ensuite être transférées sur le chemin alterné (*Alternate Path*).

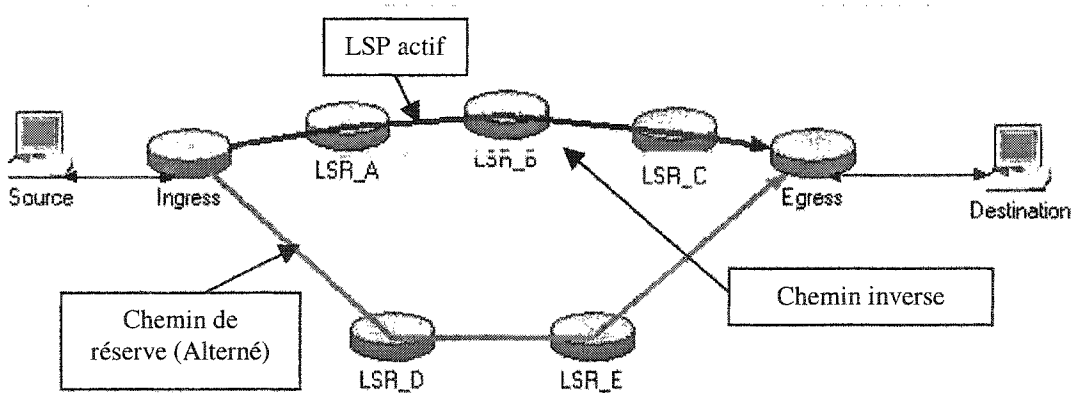

Figure 2.10 Reroutage rapide – Protection de chemin

Afin d'établir un tel chemin de protection:

- un LSP primaire doit être signalé de l'*Ingress* vers l'*Egress* ;

- un chemin inverse doit être signalé de l'*Egress* vers l'*Ingress* ;
- un chemin alterné doit être signalé de l'*Ingress* à l'*Egress* en utilisant un chemin disjoint du chemin primaire ;
- le nœud *Ingress* établit ses étiquettes de manière à ce que les informations transmises sur le chemin inverse soit toujours routées vers le chemin alterné.

Un point critique avec cette technique est la longueur du chemin de réserve à parcourir si la panne a lieu près de l'*Egress*. Si les chemins inverses et alternés sont trop longs, cela pourrait conduire à des délais de transmission inacceptables pour des trafics critiques comme la voix ou la vidéo-conférence. Une solution est représentée à la Figure 2.11. Il s'agit d'établir un chemin de raccourci (*Shortcut path*) entre le chemin primaire (protégé) et le chemin alterné. Une défaillance en amont du chemin raccourci (par exemple aux points *A* ou *B*) sera traitée telle que décrit précédemment. Par contre, lors d'une défaillance entre le chemin raccourci et le chemin inverse (par exemple aux points *C* et *D*), l'information sera acheminée au chemin alterné en passant successivement par le chemin inverse et le chemin raccourci. La même approche peut être appliquée pour des portions de chemin de manière à offrir la protection de segment.

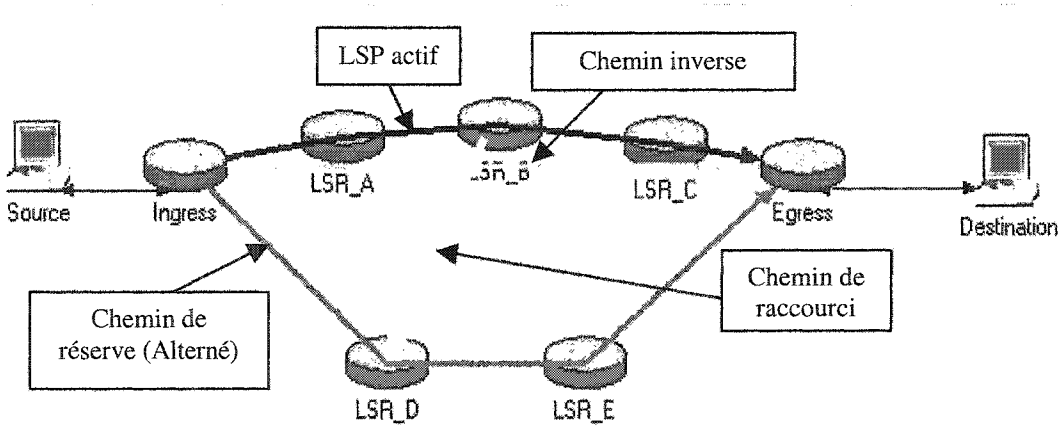

Figure 2.11 Reroutage rapide – Protection de chemin avec chemin raccourci

Chemin inverse

Un chemin inverse peut être utilisé dans une situation où la perte d'information est inacceptable. L'idée consiste à rediriger le trafic au point de défaillance du LSP protégé vers la source (*Ingress*). La source est alors responsable de commuter le trafic vers le chemin inverse aussitôt que la panne est détectée. Les avantages d'une architecture utilisant des chemins inverses sont:

- elle permet de retrouver tous les paquets en cas de panne, donc pas de pertes d'information ;
- elle simplifie la notification d'erreur car le chemin inverse peut être utilisé pour transmettre les messages FIS.

Cependant, l'utilisation de chemin inverse présente certains désavantages:

- il y a une mauvaise utilisation des ressources du réseau, puisque deux chemins (chemin inverse et chemin alterné) doivent être établis pour protéger le chemin primaire ;
- le temps requis pour acheminer les messages FIS au nœud *Ingress* peut être assez important.

2.4 Sommaire des techniques de survivabilité

Le Tableau 2.1 résume les différentes techniques présentement utilisées pour assurer la survivabilité des réseaux. Les comparaisons sont basées sur :

- la méthode de protection ;
- les ressources requises pour assurer la protection ;
- la vitesse de déclenchement de la protection ;
- la complexité de la configuration et de la signalisation ;
- la longueur du chemin de protection.

Tableau 2.1 Méthodes de protection de LSP

Méthode de protection	Ressources requises	Vitesse de déclenchement	Complexité (Configuration)	Complexité (Signalisation)	Longueur du chemin
Protection locale	Pas de réservation. Le LSP protégé utilise les ressources disponibles.	Lente. Dépend de la mise à jour des tables de routage et de la signalisation additionnelle.	Pas de configuration additionnelle.	Pas de signalisation additionnelle.	Le chemin alterné n'est pas nécessairement le chemin le plus court disponible.
Reroutage à l'Ingress	Pas de réservation. Le LSP protégé utilise les ressources disponibles.	Lente. Dépend de la mise à jour des tables de routage et de la signalisation additionnelle. Ajout de la notification d'erreur à l'Ingress.	Pas de configuration additionnelle.	Pas de signalisation additionnelle.	Le chemin alterné est le chemin le plus court de disponible.
Protection par commutation	Le LSP de réserve est réservé, mais peut être partagé par plusieurs LSP primaires.	La vitesse est limitée à la vitesse de propagation de l'erreur au point de réparation.	Le LSP de réserve doit être configuré à l'Ingress.	Les techniques de signalisation restent les mêmes, mais il faut signaliser deux LSP (primaires et *backup*).	La longueur du chemin de protection dépend de la configuration .
Reroutage rapide (Protection de lien)	Les LSP de réserve sont réservés. Un LSP de réserve pour chaque lien protégé.	Réparation rapide aussitôt que l'erreur est détectée.	Le LSP de réserve doit être configuré.	Pas de changement, mais la signalisation peut être limitée à des étiquettes globales.	La longueur du chemin primaire additionnée à la longueur du chemin alterné.

Tableau 2.1 Méthodes de protection de LSP (Suite)

Méthode de protection	Ressources requises	Vitesse de déclenchement	Complexité (Configuration)	Complexité (Signalisation)	Longueur du chemin
Reroutage rapide (Protection de nœud)	Les LSP de réserve sont réservés. Un LSP de réserve pour chaque nœud protégé.	Réparation rapide aussitôt que l'erreur est détectée.	Le LSP de réserve doit être configuré.	Les étiquettes doivent êtres reportés dans le paramètre RRO (*Record Route Object*). Peut être limité à des étiquettes globales.	La longueur du chemin primaire additionnée à la longueur du chemin alterné.
Reroutage rapide (Protection de chemin)	Plusieurs LSP sont réservés lors de la signalisation du LSP de réserve.	Réparation rapide aussitôt que l'erreur est détectée.	Les chemins inverse, alterné, et raccourcis doivent être configurés.	Additions complexes au niveau de la signalisation des chemins inverse, alterné, et raccourcis.	La longueur du chemin résultant peut atteindre jusqu'à trois fois la longueur du chemin original.

2.5 Modèle RD-QoS

RD-QoS (*Resilience-Differentiated QoS*) est un modèle étendu de qualité de service qui permet d'assigner à chaque classe de service un ensemble de mécanismes de protection appropriés (Autenrieth et Kirstädter, 2002). Cet objectif est réalisé en créant un ensemble de classes de service. Pour chaque classe de trafic, RD-QoS assignera un mécanisme de protection existant. Avec RD-QoS, les mécanismes de protection par commutation et de reroutage rapide sont assignés pour la protection des classes de trafic nécessitant un haut niveau de protection.

2.5.1 Architecture du modèle RD-QoS

Les spécifications de survivabilité sont incluses dans la signalisation de la qualité de service entre les applications et le réseau. La signalisation comprend les attributs qui identifient les requis en survivabilité des services. Les paquets appartenant à une classe donnée sont marqués en conséquence à la frontière du réseau. Dépendamment de l'architecture utilisée pour assurer la qualité de service, le marquage des paquets peut être effectué en utilisant les octets TOS de l'entête IP (*DiffServ Code Point*) ou en utilisant une étiquette MPLS spécifique ou en référant à une description de flot spécifique (IntServ, RSVP).

De plus, le réseau doit gérer la bande passante et les ressources adéquatement de manière à assurer une continuité de service pour chaque classe, et ce, même en présence de panne. Cette continuité de service est assurée en réservant suffisamment de bande passante.

2.5.2 Classification de services et schémas de résilience

Autenrieth et Kirstädter (2002) ont proposé un ensemble de quatre classes de résilience distinguées par leur temps de restauration : *Resilience Class 1 (RC1), Resilience Class 2 (RC2), Resilience Class 3 (RC3), Resilience Class 4 (RC4).*

RC1 *(Resilience Class 1)*

Le trafic assigné à cette classe possède les plus grandes exigences en terme de rapidité du temps de restauration. Dans cette classe de résilience, on s'attend à des temps de restauration inférieurs à 100 msec. Le type de protection utilisé pour le trafic assigné à la classe RC1 est la protection par commutation. Étant donné que le reroutage rapide offre des temps de restauration comparables, voire supérieurs, à la protection par commutation, il peut être utilisé dans cette classe. Les ressources de protection sont réservées pour cette classe de protection.

RC2 (*Resilience Class 2*)

Le trafic assigné à cette classe de résilience possède des requis en qualité de service modéré. Les temps de restauration visés sont de l'ordre de 100 msec à 1 seconde. Les mécanismes de protection utilisés pour restaurer le trafic sont des mécanismes de reroutage MPLS, où on tente de re-signaliser de nouveaux LSP avec les contraintes de qualité de service. Les ressources de protection ne sont pas réservées, mais les priorités de préemption sont très élevées de manière à faciliter l'acheminement du trafic par un chemin alterné.

RC3 (*Resilience Class 3*)

Le trafic assigné à cette classe de résilience possède des contraintes de qualité de service faible, et exige des temps de restauration de l'ordre de 1 sec à 10 sec. Le mécanisme utilisé pour assurer la protection de cette clase est le reroutage IP. Le reroutage a lieu seulement lorsque la restauration a été complétée pour les classes RC1 et RC2. Il n'y a pas de réservation de ressources ni de priorité de préemption pour cette classe de résilience, donc la restauration du trafic dépend de la disponibilité des ressources du réseau après la panne.

RC4 (*Resilience Class 4*)

Cette classe de résilience est définie pour les trafics n'ayant aucune contrainte de résilience. Lors d'une panne, le trafic RC4 peut être rejeté de manière à libérer des ressources pour les classes de trafic supérieures. Le Tableau 2.2 résume les caractéristiques des quatre classes de trafic RD-QoS.

Tableau 2.2 Classes de service RD-QoS et leurs options de résilience

Service class	RC1	RC2	RC3	RC4
Requis de résilience	Élevé	Moyen	Faible	Aucun
Temps de recouvrement	10 – 100 msec	100 msec – 1sec	1 sec – 10 sec	N.A.
Mécanismes de résilience	Protection	Restauration	Reroutage	Préemption
Mise en place du chemin de relève	Pré établi	Sur demande (Immédiatement)	Sur demande (Avec délai)	Aucun
Allocation des ressources	Réservé à l'avance	Sur demande (Avec garantie de disponibilité)	Sur demande (Si disponible)	Aucun
Qualité de service après le recouvrement	Equivalant	Peut être réduit temporairement	Peut être réduit	Aucun

Les classes définies au Tableau 2.2 décrivent les options de résilience pour chaque classe de service. Des attributs de résilience supplémentaires peuvent être définis pour assurer une gestion plus efficace des ressources.

2.5.3 Extension à RSVP/RSVP-TE

Pour être utilisé avec l'architecture RD-QoS, le protocole de signalisation RSVP doit être étendu de manière à permettre au terminal utilisateur de signaler ses exigences de survivabilité en plus des exigences de largeur de bande et de délai. La méthode proposée pour accomplir cette tâche est d'inclure les requis de résilience dans le paramètre *Ressource Specification* (RSpec) de RSVP. Deux bits de résilience identifiant

les classes de service seront combinés aux trois classes de IntServ (*Garanteed*, *Controlled load*, et *Best effort*).

Le réseau doit réserver les ressources adéquates de manière à assurer l'établissement d'un chemin alterné en cas de panne pour les trafics appartenant aux classes de résilience RC1 et RC2. Afin de respecter les contraintes sur le temps de restauration, il est important que le temps de détection de fautes soit de l'ordre de 10 msec.

Pour conclure cette sous section, on s'aperçoit que le modèle RD-QoS a l'avantage de proposer une protection par classes de service. Plus les trafics sont sensibles aux délais, plus ils bénéficieront des mécanismes de protection les plus coûteuses en ressources et les plus efficaces. Par contre, cette méthode a deux grandes lacunes. D'une part, elle fait appel à la protection par commutation, qui dépend de ressources réservées à l'avance. Donc, il y a sous-optimisation des ressources pour les classes de trafic RC1. Ensuite, le temps de restauration pour la classe RC1, qui devrait comprendre le trafic de voix, se situe dans un intervalle de 10 à 100 msec. Donc, il n'y a aucune garantie que le temps de restauration sera inférieur à 50 msec. Or, l'objectif de notre travail de recherche est d'assurer un temps de restauration inférieur à 50 msec pour la voix. L'idée de reroutage par chemins alternés est intéressante, puisque les ressources ne sont pas réservées. Cependant, les LSP sont calculés lors d'une panne, ce qui implique qu'il est impossible de garantir une restauration à l'intérieur de 50 msec. C'est pourquoi on utilise le reroutage par chemins alternés pour la classe RC2, et non la classe RC1. Cette approche nous lance sur une bonne piste, celle des classes de résilience, mais il reste encore du raffinement pour atteindre les objectifs du TE tout en assurant un haut niveau de protection et une restauration rapide aux classes de trafic qui le requiert.

2.6 Conclusion

Pour résumer, nous avons présenté un survol rapide des fonctionnalités de gestion de fautes qui sont présentement disponible sur MPLS, ainsi que les mécanismes de protection tel le reroutage rapide et la protection par commutation. Nous avons aussi exploré le modèle RD-QoS, qui permet de combiner les mécanismes de restauration existante de manière à assurer une protection efficace basée sur des classes de résilience.

Il est intéressant de constater que les approches de *Protection Switching* et de *Fast Reroute* offrent des temps de complétion rapide, mais ils n'optimisent pas les ressources du réseau puisque les chemins de réserve sont réservés pour la protection. Il apparaît donc opportun de développer des méthodes de restauration qui minimiseront le nombre de chemins réservés tout en offrant un temps de complétion et une qualité de service comparable à la protection par commutation et au reroutage rapide. Dans le prochain chapitre, on explorera un modèle de protection qui combine les différents mécanismes existant afin d'assurer la protection par classe de trafic.

CHAPITRE III
ROUTAGE ALTERNÉ PROACTIF BASÉ SUR LA QUALITÉ DE SERVICE UMTS

L'expansion de l'Internet semble favoriser le déploiement de réseaux MPLS. Afin d'assurer la fiabilité de ces réseaux, les opérateurs utilisent les fonctionnalités de gestion des fautes disponibles avec le protocole MPLS. Ces fonctionnalités sont utilisées pour implanter les mécanismes de protection tels la *Protection par Commutation* (*Protection Switching*) et le *Reroutage Rapide* (*Fast-Reroute*). Cependant, ces mécanismes reposent sur la réservation de ressources, ce qui induit une sous-optimisation des ressources du réseau, puisqu'on doit surdimensionner. L'autre approche proposée est le routage alterné qui offre le bénéfice de ne pas réserver de ressources, mais le temps de complétion est plus long puisque les chemins alternés sont calculés uniquement après la notification de la panne. Pour des trafics comme la voix et la vidéo-conférence, le délai de calcul engendré est souvent inacceptable puisque le temps de restauration doit être inférieur à 50 msec. C'est pourquoi nous proposons une solution basée sur le routage alterné, mais qui calculera les chemins de réserve avant une panne. Cette approche se nomme *Proactive Alternate Routing for UMTS* (PAR-UMTS). Dans ce chapitre, nous examinons tout d'abord la motivation et les fondements de l'approche PAR-UMTS. Ensuite, nous présenterons l'architecture, puis décrirons le prototype réalisé. Par la suite, nous donnerons des détails d'implémentation du prototype. Le chapitre se termine par une synthèse des problèmes ouverts.

3.1 Motivation et fondements

Avec les approches conventionnelles, protection locale ou globale, la survivabilité est assurée par un surdimensionnement des ressources du réseau, ce qui permet un temps de restauration de 50 msec pour les trafics critiques comme la voix. Nous examinerons la motivation à assurer la survivabilité à l'aide d'un protocole de routage proactif qui ne

requiert pas de réservation de ressources. Par la suite, nous présenterons les bénéfices de cette approche.

3.1.1 Motivation

La motivation derrière cette approche est d'ordre qualitatif. Il s'agit d'offrir les mêmes garanties de temps de réponse que les méthodes *Protection par Commutation* et de *Reroutage Rapide* lors d'une panne, en évitant de réserver des ressources. Le gain de l'approche vient du fait que les ressources qui étaient auparavant réservées servent maintenant à transmettre du trafic utile, et à optimiser les revenus générés par l'exploitation du réseau. Cette approche se veut donc une extension et une amélioration du *Reroutage Rapide* et de la *Protection par Commutation*. Cette garantie de temps de réponse rapide, on compte l'obtenir en gardant en mémoire les informations de routage pour le LSP de réserve avant la détection d'une panne. C'est d'ailleurs l'élément qui permet aux méthodes de *Protection par Commutation* et de *Reroutage Rapide* d'offrir un temps de complétion rapide.

De façon générale, le temps de complétion peut être exprimé en fonction des paramètres suivants :

C : Temps de complétion

D : Temps de détection par le PLR le plus près

N : Temps de notification (envoi du message de notification à l'Ingress)

R : Temps de calcul d'une nouvelle route

E : Temps d'établissement de la route r (signalisation)

S : Temps de commutation (*Switching*) du trafic du LSP initial au LSP calculé

Pour le routage alterné, on aura :

$$Cr = D + N + R + E + S \qquad (\textit{Routage alterné})$$

Dans le cas des méthodes *Protection par Commutation* et *Reroutage Rapide*, le fait que les chemins de réserve soient connus et réservés à l'avance, le temps de calcul

(R) et d'établissement (E) des LSP sont nuls ($R = 0$ et $E = 0$). Le temps de complétion est donc donné par :

$C_{PF} = D + N + S$ (*Protection Switching* et *Fast Reroute*)

Or, dans le cas d'un réseau à taux d'utilisation normal (40 à 60 %) des liens, on a : $R >> D$, $R >> N$, $R >> E$, et $R >> S$.

La rapidité de ces deux méthodes est due au fait que le temps de calcul (R) et d'établissement (E) des LSP sont négligeables ($R = 0$ et $E = 0$). Nous estimons que le temps de réponse de notre approche sera de :

$C_P = D + N + S$ (PAR-UMTS)

On peut donc conclure que : $C_P = C_{PF}$

L'avantage de notre approche est que, contrairement aux mécanismes de *Protection par Commutation* et *Reroutage Rapide*, il n'y a pas de réservation de ressources. Donc, le prix à payer pour obtenir un temps de réponse rapide est très faible, dans la mesure où il existe un chemin alterné. Maintenant, vu l'hypothèse de bi-connexité des chemins, la probabilité de trouver un chemin alterné est plutôt élevée, sans être garantie à 100 %.

3.1.2 Fondements de l'approche PAR-UMTS

Plusieurs cas de figure sont à considérer pour implanter l'approche PAR-UMTS. D'abord, tous les nœuds du réseau peuvent se trouver ou non dans un même domaine administratif. Ensuite, il peut y avoir une pluralité de trafics sur le réseau, i.e. UMTS, WLAN, PSTN, etc. Finalement, la restauration de trafic peut être enclenchée soit par l'Ingress, un ou plusieurs nœuds intermédiaires ou par l'Ingress et des nœuds intermédiaires.

Dans ce mémoire, nous adoptons les hypothèses suivantes :

- la restauration/protection de trafic a lieu au nœud Ingress ;
- tous les nœuds du réseau font partie du même domaine administratif ;
- seuls les trafics de la classe conversationnelle et le trafic de données seront considérés dans le modèle ;

- l'approche ne fait pas intervenir de réservation, mais plutôt des priorités de préemption et de rétention de ressources. Ces priorités sont accordées dans l'ordre aux trafics suivants : voix, vidéo-conférence, vidéo sur demande (*Streaming*), et données ;
- l'approche doit assurer un temps de complétion inférieur à 50 msec et un délai de bout en bout inférieur à 150 msec ;
- l'algorithme de routage utilisé sera un algorithme 'état de lien' CSPF, i.e. OSPF avec contraintes ;
- le taux d'utilisation des liens en temps normal varie de 40 % et 60 % ;
- le trafic du réseau est stable à l'intérieur de l'intervalle ΔT des simulations. Nous considérerons qu'il appartient à l'opérateur de réseau de décider des fréquences de mise à jour des chemins alternés.

Ce mémoire se concentre donc sur la réalisation d'une approche de protection/restauration globale. La restauration locale fera l'objet d'une extension à nos travaux. Cependant, le modèle proposé tiendra compte des protections globale et locale.

Scénario d'illustration

Tout d'abord en accès, on retrouve des usagers UMTS, WLAN et PSTN. Sur le réseau dorsal, les protocoles utilisés sont IP et MPLS. La dorsale comprend un seul domaine administratif. De plus, on pose l'hypothèse de la bi-connexité des chemins transportant la voix et la vidéo-conférence.

Bénéfices attendus

Les principaux bénéfices attendus de notre approche sont :

1. Optimisation des ressources et des revenus d'exploitation

L'approche ne nécessite pas la réservation de ressources de réserve en cas de panne. Elle tente plutôt de chercher un chemin disponible qui satisfait les contraintes de

QoS. Elle se base donc sur la capacité résiduelle des liens pour établir un chemin à utiliser en cas de panne. Ce chemin est ensuite sauvegardé dans la mémoire cache du routeur Ingress. Lors d'une panne, le routeur Ingress transfère le trafic sur le chemin alterné après avoir reçu un message de notification de panne. Le fait que les ressources ne soient plus réservées entraîne aussi une augmentation des revenus d'exploitation du réseau, puisque les chemins qui étaient jadis réservés à la protection peuvent maintenant être utilisés pour offrir des services payants.

2. Indépendance de l'équipement et du réseau d'accès

L'accès au réseau n'est pas restreint à un seul type d'équipement. L'usager peut accéder au réseau via n'importe quel terminal. Les équipements du réseau d'accès n'influencent pas le fonctionnement de l'approche. De plus, l'approche s'adapte facilement à tous les réseaux d'accès puisqu'il suffit de définir un certain nombre de classes de trafic et leur accorder des priorités de préemption et de rétention des ressources.

3.2 Modélisation de l'approche *PAR-UMTS*

Dans cette section, nous décrivons l'approche proposée pour assurer la survivabilité des réseaux dorsaux IP/MPLS, ainsi que les hypothèses sur lesquelles repose notre raisonnement. En effet, il s'agit d'un algorithme de reroutage qui calcule à l'avance les chemins alternés à emprunter en cas de panne pour chaque LSP d'un réseau IP/MPLS. C'est un algorithme de routage proactif, c'est à dire qu'il calcule les routes à l'avance et non sur demande. Les chemins calculés sont stockés, et utilisés au besoin.

Cette approche s'applique pour un réseau de type dorsal multiservice IP/MPLS. Les réseaux d'accès peuvent être divers : des accès WLAN, UMTS, PSTN, etc. Dans le cadre de notre mémoire, nous centrerons les efforts sur un réseau d'accès de type UMTS qui définit quatre classes de services ayant chacune des caractéristiques et des contraintes de qualité de service particulières. On retrouve la classe *Conversational* qui comprend la voix et la vidéo-conférence interactive. Ensuite, il y a la classe *Streaming* qui comprend

la vidéo sur demande. La troisième classe est la classe *Interactive* qui inclut le *Web Browsing*, l'accès aux bases de données (*data base retrieval*), l'accès à des serveurs (*server access*). Finalement, le trafic de courrier électronique est inclus dans la classe *Background.*

De plus, on considère que le réseau dorsal fait partie d'un seul et unique domaine administratif. Cette hypothèse induit les considérations suivantes. D'abord, le nombre de nœuds est compris entre 10 et 15. Afin d'assurer l'existence d'un chemin alterné, on considère que les LSP contenant les trafics *Conversational* et *Streaming* doivent être bi-connexes entre l'Ingress et l'Egress. Dans le cas du trafic de la classe *Interactive*, on utilisera directement des LSP de type *Background*, s'il n'existe pas plus de LSP de ce type lors du calcul de chemin alterné pour fin de restauration.

Une autre hypothèse touche l'utilisation des liens. Dans les WAN des fournisseurs de service et des grandes entreprises, il est pratique courante d'utiliser la capacité des liens à un taux variant entre 40 et 60 % en temps normal, en plus de prévoir des ressources de réserve en cas de pannes. Dans notre approche, nous conserverons ces taux d'utilisation; par contre, il n'y aura pas de réservation de ressources additionnelles.

Nous croyons que l'algorithme offrira des performances convaincantes pour les raisons suivantes :

- nous utiliserons comme protocole de routage le protocole CSPF. C'est un protocole de type «état de lien» qui permet à chaque nœud du réseau d'avoir une vision exacte de la topologie. CSPF est basé sur OSPF et calcule les routes en tenant compte des différentes contraintes telles la bande passante résiduelle, le délai de transmission, le coût des liens, etc. ;
- l'approche PAR-UMTS utilisera les informations fournies par le protocole CSPF pour calculer les chemins alternés après un changement de topologie. Les chemins calculés par CSPF seront sauvegardés dans la mémoire cache du routeur Ingress. Le fait de sauvegarder les chemins alternés en mémoire cache contribuera à réduire le temps de restauration au même niveau que celui de *Protection par*

Commutation ou du *Reroutage* Rapide. La rapidité de ces deux méthodes est due au fait que les chemins alternés sont déjà en mémoire bien avant la panne.

L'implémentation de l'approche se fera sur OPNET et reposera sur quatre composants :

1- un algorithme de routage avec contraintes qui calcule les chemins alternés en tenant compte des contraintes de chaque trafic ;
2- un mécanisme qui permet la sauvegarde des résultats du calcul dans la mémoire cache du routeur de tête (Ingress) ;
3- un mécanisme de détection et de notification de fautes qui prévient le nœud Ingress qu'une panne a eu lieu ;
4- un mécanisme de commutation permettant au routeur de tête (Ingress LER) de sélectionner le chemin alterné approprié et de commuter le trafic sur ce chemin.

3.3 Prototypage

Le prototype bâti pour démontrer la faisabilité de la solution repose sur les hypothèses suivantes:

- la protection du trafic sera globale, c'est à dire que les LSP seront protégés du nœud Ingress au nœud Egress; et c'est le nœud Ingress qui enclenchera le processus de restauration ;
- la topologie du réseau offre une bi-connexité pour les chemins *Conversational et Streaming*.

3.3.1 Environnement expérimental

L'environnement expérimental est un ordinateur de bureau Pentium IV muni du logiciel de simulation OPNET Modeler 9.0. Dans ce logiciel, nous ferons une extension du modèle MPLS_Fast_REROUTE disponible afin de tester notre proposition.

3.3.2 Principaux éléments à considérer dans le prototype

Gestion de la largeur de bande

La gestion de la largeur de bande consiste à gérer les ressources du réseau MPLS de manière à respecter les contraintes de qualité de service pour chaque type de trafic. Cette fonction comprend la signalisation des LSP et le dimensionnement, les priorités de préemption, et l'allocation de capacité.

La signalisation du LSP peut se faire soit à l'avance ou sur demande lorsqu'on doit acheminer un trafic. Les priorités de préemption déterminent si un LSP ayant une certaine priorité peut avoir un accès prioritaire à un chemin sur un autre LSP ayant une priorité plus faible. On utilise les priorités de préemption pour assurer que les trafics appartenant à une classe de trafic supérieure (par exemple *Conversational*) auront toujours un accès prioritaire aux ressources du réseau. Lors de l'établissement d'un LSP, les deux paramètres importants à spécifier sont la largeur de bande requise et la priorité de préemption.

L'allocation de la capacité peut se faire de façon statique ou dynamique. L'allocation statique assigne la largeur de bande avant la transmission de données. Si cette approche est simple pour l'allocation, elle entraîne un gaspillage de ressources. L'allocation dynamique renégocie périodiquement l'assignation de largeur de bande. Cette approche est plus efficace en terme d'optimisation des ressources, mais elle demande plus de signalisation. L'approche idéale serait de procéder à une allocation dynamique dans l'implémentation de notre prototype, mais pour fins de simplicité, l'allocation statique sera utilisée. L'allocation dynamique fera l'objet d'extension à notre travail.

Gestion des chemins

La gestion des chemins consiste à trouver des chemins servant à router les LSP sur le réseau MPLS. Ce processus est déclenché lorsque l'Ingress qui reçoit une requête pour établir un LSP, doit allouer des capacités ou lorsque l'Ingress reçoit un message de notification de panne et doit établir un chemin alterné. L'approche la plus efficace pour

gérer les routes serait d'utiliser un algorithme de routage dynamique qui tient compte du trafic en temps réel du réseau de manière à établir des chemins de réserve optimaux. Afin de simplifier le problème, on utilisera l'algorithme CSPF dans le prototype, en prenant l'hypothèse que le trafic est constant.

3.4 Implémentation

Cette section présente une analyse structurée de l'implémentation de l'approche PAR-UMTS. Nous analyserons les principaux éléments à considérer dans l'implémentation de l'approche.

3.4.1 Architecture

La Figure 3.1 illustre les principales composantes de l'architecture PAR-UMTS. On retrouve d'abord la base de données de topologies qui contient les chemins empruntés par les LSP. Le protocole de routage qui sert à calculer les chemins que doivent emprunter les LSP en tenant compte des contraintes liées aux trafics. De plus, les protocoles de signalisation sont utilisés pour gérer l'établissement, le maintien et la suppression des LSP. On retrouve aussi une table de routage qui sert à sauvegarder les informations sur les chemins primaires et les chemins alternés. Le paradigme de qualité de service peut être *DiffServ* ou *Integrated Service*. Finalement, il y a l'outil de gestion et d'ingénierie de trafic qui fait appel aux autres composantes pour calculer, réserver et accorder les priorités de préemption sur les chemins et LSP. Ce module s'occupe aussi de gérer la signalisation, l'allocation des capacités, la détection et la notification de pannes, la commutation du trafic et le calcul de nouveaux chemins alternés après la commutation du trafic.

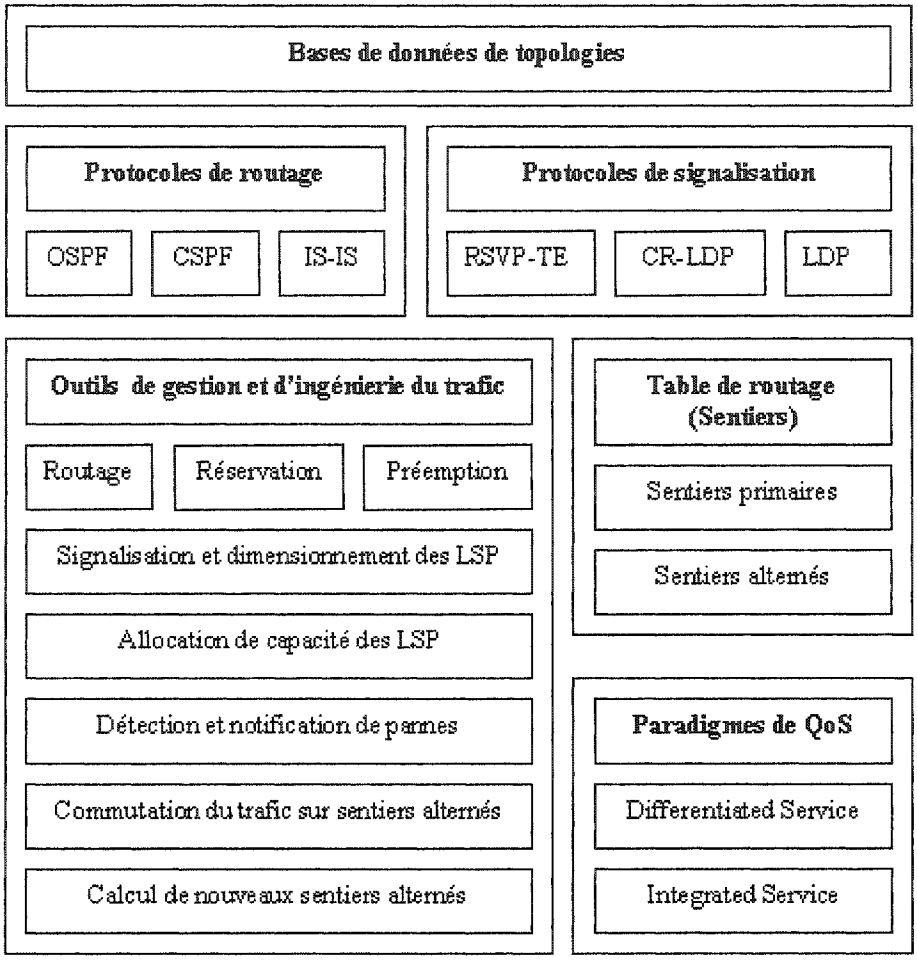

Figure 3.1 Architecture de l'algorithme PAR-UMTS

3.4.2 Algorithme

L'algorithme à utiliser lors de l'initialisation des LSP et lors des mises à jour est illustré à la Figure 3.2.

Lors de la signalisation initiale des LSP et lors des mises à jour de la table:
Pour chaque classe de trafic :
- Calculer un/des chemins alternatifs qui peuvent être utilisés en cas de panne
  - Si le chemin alterné est un autre chemin possible pouvant router le LSP, alors l'indiquer dans la table.
  - Sinon, il faut utiliser un autre LSP existant.
    - S'il n'existe pas un LSP capable d'accommoder tout le trafic en cas de panne :
      - Effectuer l'équilibrage de charge (*Load Balancing*), ou
      - Utiliser un LSP avec QoS d'une classe inférieure si nécessaire.
- Sauvegarder les résultats du calcul dans la mémoire cache du LSR.

Figure 3.2 Algorithme (Lors de la signalisation initiale)

Lors d'une panne, on utilisera la procédure décrite à la Figure 3.3.

Lors de la notification d'un changement topologique :
Pour chaque classe de trafic affectée par le changement :
- Consulter la table des chemins alternatifs contenue dans la mémoire cache
- S'il est possible de rerouter le trafic sur un autre chemin appartenant au LSP,
  - Re-router le trafic
  - Mettre à jour la table de chemins alternés
- Sinon, on vérifie qu'il existe un LSP de la même classe avec assez de ressources pour prendre en charge le trafic
  - Commuter le trafic sur ce LSP
  - Mettre à jour la table de chemins alternés
- Sinon, on vérifie qu'il existe un LSP d'une classe inférieure avec assez de ressources pour prendre en charge le trafic
  - S'il y a du trafic d'une classe inférieure sur ce LSP, la priorité est donnée à la classe de trafic supérieure
  - Mettre à jour la table de chemins alternés
- Sinon, il faut signaliser un nouvel LSP
  - Signaliser le LSP alterné en se basant sur les informations de la table
  - Commuter le trafic sur le nouvel LSP
  - Mettre à jour la table de chemins alternés.

Figure 3.3 Algorithme (Lors d'un changement de topologie)

3.4.3 Établissement de LSP de réserve avec RSVP-TE

Le premier élément à considérer dans l'implémentation d'un modèle de réseau MPLS est le protocole de signalisation. C'est ce protocole de signalisation qui permet d'établir les LSP, en tenant compte des besoins et des contraintes en terme de qualité de service. Le protocole de signalisation assurera la gestion de la largeur de bande et des chemins, et offrira les fonctionnalités pour signaler les pannes et enclencher les mécanismes de protection.

Trois protocoles de signalisation peuvent être utilisés afin d'établir des LSP: RSVP, CR-LDP, et LDP. Dans cette section, nous expliquerons en détails l'utilisation du protocole RSVP-TE et les extensions qui lui ont été apportées pour établir des LSP, puisque c'est le protocole que l'IETF a choisi pour implémenter le *Reroutage Rapide* et la protection locale. Nous allons aussi étendre son utilisation à la protection globale dans le cadre de l'approche PAR-UMTS.

Extension à RSVP

Afin de pouvoir accommoder RSVP pour le *Reroutage Rapide*, deux nouveaux objets ont été ajoutés : FAST_REROUTE et DETOUR. Ces objets sont donnés sous forme de TLV (*Type Length Value*) et ils sont transportés dans le message RSVP_Path. De plus, des extensions ont été apportées aux objets SESSION_ATTRIBUTE et RECORD_ROUTE de manière à supporter des fonctionnalités pour la largeur de bande et la protection de nœud. Nous utiliserons ces objets dans l'implémentation de PAR-UMTS.

3.4.3.1 Objet FAST_REROUTE

Un LSP protégé utilise l'objet FAST-REROUTE pour indiquer le niveau de protection requis lors de la protection locale ou pour identifier un LSP pré-déterminé sur le réseau d'un fournisseur de service. Cet objet transporte les informations de contrôle, tel que les priorités d'établissement et de rétention (*Setup Priority and Hold Priority*) ainsi que les priorités sur la largeur de bande.

Les paramètres inclus dans l'objet FAST_REROUTE sont décrits au Tableau 3.1.

Tableau 3.1 Paramètres de l'objet Fast-Reroute

Paramètres	Descriptions
Priorité de signalisation (*Setup Priority*)	Identifie le niveau de priorité du chemin de réserve à prendre par les ressources. Il est utilisé pour décider si la session courante a priorité sur une autre session.
Priorité de rétention (*Holding Priority*)	Identifie le niveau de priorité du chemin de réserve à garder des ressources. Il est aussi utilisé pour décider si la session courante a priorité sur une autre session.
Nœud limite (*Hop-limit*)	Identifie le nombre maximum de routeurs supplémentaires que le chemin de réserve a le droit d'utiliser entre le PLR courant et le MP, le PLR et le PM étant exclus.
Drapeau (*Flags*)	Indique le type de protection désiré: (Protection 1 : 1) ou (Protection n : 1).
Largeur de bande (*Bandwidth*)	Identifie l'estimation de largeur de bande en octets par seconde.
Exclusion (*Exclude-any*)	Un vecteur de 32-bits qui représente un ensemble d'attributs associés à un chemin de réserve, n'importe lequel de ces attributs pouvant rendre un lien inacceptable.
Inclusion partielle (*Include-any*)	Un vecteur de 32-bits qui représente un ensemble d'attributs associés à un chemin de réserve, n'importe lequel de ces attributs pouvant rendre un lien acceptable.
Inclusion complète (*Include-all*)	Un vecteur de 32-bits qui représente un ensemble d'attributs associés à un chemin de réserve, tous ces attributs doivent être présents pour rendre un lien acceptable.

3.4.3.2 Objet DETOUR

L'objet DETOUR est utilisé uniquement dans la *Protection 1 : 1* pour établir et identifier les LSP de détour. Contrairement au reroutage traditionnel, le détour n'est pas un LSP réservé uniquement pour fins de protection, mais un LSP ou une portion de LSP primaire qui sera utilisé comme LSP alterné en cas de panne. Pour le calcul de la largeur de bande disponible, on tiendra compte de la capacité résiduelle du chemin. Cette capacité sera égale à la plus petite capacité disponible sur un lien du chemin. Deux paramètres sont importants dans l'objet DETOUR :

- *PLR ID (1 - n)* : identifie l'adresse IPv4 du point PLR qui correspond à l'origine du détour ;

- *Avoid Node ID (1 - n)* : identifie l'adresse IP du prochain nœud en aval que le PLR essaie d'éviter. Ce champ est obligatoire.

Il est à noter que plus d'une paire (*PLR ID*, *Avoid Node ID*) peut être disponible en entrée dans l'objet DETOUR.

3.4.3.3 Modification à l'objet SESSION_ATTRIBUTE

Afin d'effectuer une requête explicite en largeur de bande et en protection de nœud, deux nouveaux paramètres (*Flags*) ont été définis dans l'objet SESSION_ATTRIBUTE. Une description des paramètres existant et des nouveaux paramètres proposés par l'IETF est donnée au Tableau 3.2.

Tableau 3.2 Paramètres de l'objet SESSION_ATTRIBUTE

Type de paramètres	Nom	Valeur	Description
Existant	Protection locale désirée (*Local Protection desired*)	0x01	Ce paramètre permet aux routeurs de transits d'utiliser un mécanisme de protection local, ce qui peut résulter en une violation du ERO.
Existant	Enregistrement d'étiquettes désiré (*Label recording desired*)	0x02	Ce paramètre indique que les informations sur les étiquettes doivent être incluses lorsqu'on enregistre une route.
Existant	Destruction du tunnel (*SE Style desired*)	0x04	Ce paramètre indique que le nœud du tunnel *ingress* peut choisir de rerouter ce tunnel sans le détruire.
Nouveau	**Protection de lien désirée (*Bandwidth protection desired*)**	**0x08**	Ce paramètre indique au PLR sur le chemin de protection qu'un chemin de réserve avec une garantie de largeur de bande est désiré.
Nouveau	**Protection de nœud désirée (*Node protection desired*)**	**0x10**	Ce paramètre indique au PLR sur le chemin de protection qu'ils doivent sélectionner un chemin de réserve qui évite au moins le prochain nœud du LSP protégé.

3.4.3.4 Modification à l'objet RRO

Afin de sauvegarder les informations sur la largeur de bande et la protection de nœud, deux nouveaux paramètres ont été définis dans l'objet RRO (*Record Route Object*). Une description de ces paramètres est donnée au Tableau 3.3.

Tableau 3.3 Paramètres de l'objet RECORD_ROUTE_OBJECT

Type de paramètres	Nom	Valeur	Description
Existant	Protection locale disponible (*Local Protection available*)	0x01	Indique que le lien en aval (*downstream*) de ce nœud est protégé par un mécanisme de protection locale, qui peut être *one-to-one* ou *facility backup*.
Existant	Protection locale en utilisation (*Local Protection in use*)	0x02	Indique qu'un mécanisme de protection locale est en utilisation pour maintenir ce tunnel (dû à une panne de nœud ou de lien).
Nouveau	**Protection de lien (*Bandwidth protection*)**	**0x04**	Le PLR règle ces paramètres lorsque le LSP protégé a un chemin de réserve qui offre la largeur de bande désirée, qui peut correspondre à celle contenue dans l'objet FAST_REROUTE ou qui correspond à la bande passante de chemin protégé si l'objet FAST_REROUTE n'est pas inclus.
Nouveau	**Protection de nœud (*Node protection*)**	**0x08**	Indique que le PLR a un chemin de réserve qui offre la protection contre un bris de lien ou de nœud.

3.4.4 Signalisation du chemin alterné

Un certain nombre d'objectifs doit être atteint de manière à obtenir une solution satisfaisante. Ces objectifs sont :

1. trouver des chemins de réserve (alternés) qui respectent les contraintes de qualité de service ;
2. la capacité à identifier les chemins alternés de façon unique et sans ambiguïté ;
3. associer les LSP protégés à leurs LSP de réserve (alterné) sans ambiguïté ;

4. travailler avec des espaces d'étiquettes, autant global que non-global ;
5. permettre la fusion des chemins de réserve ;
6. maintenir l'état RSVP pendant et après le *fail-over*.

Une combinaison des objets SESSION et SENDER_TEMPLATE est utilisée pour identifier les tunnels LSP. Une description de ces paramètres est donnée au Tableau 3.4.

Tableau 3.4 Paramètres identifiant un tunnel LSP

Paramètres	Descriptions
Adresse du noeud Egress (*Ipv4 tunnel end point address)*	Spécifie l'adresse IP du nœud *Egress* du tunnel.
Identifiant du tunnel (*Tunnel ID*)	L'identifiant du tunnel. Un identifiant de 16-bits utilisé dans l'objet SESSION et qui demeure constant pendant la durée de vie du tunnel.
Identifiant du tunnel étendu (*Extended Tunnel ID*)	Un identifiant de 32-bits utilisé dans l'objet SESSION et qui demeure constant pendant la durée de vie du tunnel. Il est normalement réglé à zéro. Les nœuds *Ingress* qui veulent limiter l'étendue de l'objet SESSION à la paire *Ingress-Egress* peuvent placer leurs adresses IPv4 comme identifiant global.
Adresse Ipv4 du nœud source (*IPv4 tunnel sender address*)	L'adresse IPv4 du nœud source (expéditeur).
Identifiant du LSP (*LSP ID*)	Un identifiant de 16-bits utilisé dans les objets SENDER_TEMPLATE et FILTER_SPEC, qui peut être changé pour permettre au nœud expéditeur de partager des ressources avec lui-même.

Les trois premiers paramètres sont inclus dans l'objet SESSION et les deux derniers font partie de l'objet SENDER_TEMPLATE.

Afin d'identifier les chemins de réserve, l'approche *Path Message Specific* est utilisée. Selon cette approche, les chemins alternés (de réserve) utilisent les mêmes objets SESSION et SENDER_TEMPLATE que ceux utilisés dans le LSP protégé. Cependant, les messages *Path* doivent fournir suffisamment d'informations pour permettre aux LSR de différencier les chemins de réserve des chemins protégés. La référence à ces chemins alternés est sauvegardée dans la mémoire cache du LSR Ingress.

3.4.5 Protection d'un chemin primaire par un seul chemin alterné

Cette section décrit la méthode qui permet la protection de plusieurs LSP contre des pannes de nœuds ou de liens par un seul LSP alterné.

3.4.5.1 Survol des opérations

Si un LSP est nécessaire pour assurer la protection d'un LSP primaire, alors le LSR de tête doit insérer un objet FAST_REROUTE dans le message *Path*, en prenant soin d'activer le paramètre « *One-to-one Backup desired* ». La protection peut aussi être assurée en se basant sur une politique PLR si le paramètre « *local protection desired* » est activée dans l'objet SESSION_ATTRIBUTE ou si un objet FAST_REROUTE est inclus ou les deux.

Ensuite, le LSR qui initie un LSP de détour doit pouvoir supporter les deux objets FAST_REROUTE et DETOUR. Si un LSR ne supporte pas ce standard, il ne sera pas en mesure d'établir de la protection pour des nœuds ou des liens immédiats. Dans ce cas, c'est le LSR qui est en mesure de supporter ce standard qui devra assurer le déclenchement du mécanisme de protection.

Au point MP, les LSP alternés doivent se fusionner avec les LSP protégés selon les règles de fusion définies par Braden et al. (1997) pour le paramètre *SE style reservation.*

Dans le cas ou un LSP est utilisé pour protéger plusieurs LSP, il n'est pas nécessaire que le PLR connaisse les étiquettes utilisées aux différents MP.

3.4.5.2 Procédures pour les PLR

Lorsque le PLR reçoit le message *Path* qui contient l'objet FAST_REROUTE, il doit établir une route de détour à l'aide du protocole CSPF en se basant sur les informations provenant de l'objet FAST_REROUTE, de l'interface en aval (*downstream*) et de l'information du prochain hop fourni par le routeur.

Une fois que le détour a été calculé et sauvegardé en mémoire, le PLR n'a plus besoin de l'établir à nouveau, à moins que le contenu de l'objet FAST_REROUTE change ou que l'interface en aval et/ou le prochain routeur du LSP protégé change ou qu'il y ait un changement de topologie.

Lors d'une panne, il y a deux possibilités : soit que le trafic est routé sur un autre chemin appartenant au LSP ou que le PLR signale un nouvel LSP pour rerouter le trafic.

Si un nouvel LSP est requis, le PLR consulte sa mémoire cache et génère un message *Path* pour établir un chemin alterné basé sur le contenu de sa table. Le message *Path* contient les informations suivantes :

- un objet DETOUR, qui spécifie le PLR_ID et Avoid_Node_ID courant. Seule une paire (PLR_ID, Avoid_Node_ID) est permise ;
- un objet EXPLICIT_ROUTE vers l'Egress. L'information contenue dans le ERO provient du calcul effectué par le protocole CSPF ;
- un objet SENDER_TSPEC qui contient les informations obtenues du dernier objet FAST_REROUTE sur la largeur de bande ;
- un objet RSVP_HOP qui contient l'adresse IP du PLR ;
- le LSP de détour peut générer et traiter son propre RRO ;
- l'objet FAST_REROUTE ne doit pas être inclus ;
- lorsque l'approche *Sender-template-specific* est utilisée, le paramètre « *IPv4 tunnel sender address* » de l'objet SENDER_TEMPLATE doit prendre la valeur d'une adresse IP appartenant au PLR ;
- le LSP de détour doit utiliser le même paramètre *reservation style* que le LSP protégé. Cela doit se refléter dans l'objet SESSION_ATTRIBUTE ;
- tous les autres objets doivent être identiques à ceux du LSP protégé.

3.4.6 Protection de plusieurs chemins primaires par un seul chemin alterné

Dans cette section, nous décrirons comment un seul chemin alterné peut être utilisé pour protéger plusieurs LSP. Le processus de *PAR-UMTS* est initié au LSR Ingress en donnant les bonnes valeurs aux paramètres des objets SESSION_ATTRIBUTE et/ou

FAST_REROUTE. À chaque PLR, un tunnel alterné est choisi pour rerouter les paquets de données d'un LSP en cas de panne. Lorsqu'une panne a lieu, le PLR envoie le trafic de chaque LSP protégé ainsi que les messages de contrôle sur le tunnel de réserve.

3.4.6.1 Découverte des étiquettes en aval

Le PLR peut prendre connaissance des étiquettes du chemin alterné lorsque des étiquettes globales sont utilisées au MP, en observant le contenu de l'objet RRO dans le message *Resv*. Deux méthodes sont disponibles pour découvrir/obtenir les étiquettes utilisées aux nœuds fusionnés (*Merge node*). La première méthode repose sur la signalisation explicite du tunnel de réserve avant une défaillance du chemin de protection; la seconde repose sur le contenu de l'objet RRO si les nœuds dans le réseau utilisent un espace d'étiquettes dit *global-to-the-node*.

3.4.6.2 Procédures initiales du PLR

Les étapes suivantes doivent être effectuées par le PLR sur le chemin lorsqu'un LSP protégé est établi pour la première fois:

- le PLR doit sélectionner ou créer un tunnel de réserve pour le LSP protégé si le bit « *Local protection desired* » de l'objet SESSION_ATTRIBUTE est activé et qu'aucun objet FAST_REROUTE existe ou encore, si un objet FAST_REROUTE existe avec le paramètre « *Facility-Backup-Desired* » activé ;
- le PLR doit, s'il ne peut trouver le tunnel de réserve NNHOP, activer le bit « *Node protection* » et le paramètre « *Local protection available* » de son objet RRO si l'objet RRO est inclus dans le message *Resv* ;
- le PLR doit re-initialiser (*clear*) le bit « *Node Protection* » et il doit activer le paramètre « *local protection available* » dans le RRO du message *Resv* ;
- le PLR doit activer le paramètre "*Bandwidth protection*" du RRO, s'il existe un tunnel de réserve qui garantit la largeur de bande ;
- le PLR doit re-initialiser (*clear*) le paramètre "*Bandwidth protection*" du RRO, s'il ne peut trouver un tunnel de réserve qui garantit la largeur de bande requise.

3.4.6.3 Procédures du PLR pendant la protection

Durant le processus de protection, le tunnel de réserve est identifié de la manière suivante :

- les paramètres de l'objet SESSION_ATTRIBUTE restent inchangés ;
- l'adresse source du tunnel IPv4 de l'objet SENDER_TEMPLATE est modifié (elle est réglée à une adresse qui appartient au PLR) ;
- l'objet RSVP_HOP doit contenir l'adresse source IPv4 du tunnel de réserve ;
- le PLR doit générer l'objet EXPLICIT_ROUTE vers le nœud Egress ;
- l'objet RRO doit être mis à jour ;
- toutes les informations précédentes sont partagées entre le LSR Ingress et le PLR.

3.4.6.4 Maintenance de l'état durant le fonctionnement du réseau

La maintenance de l'état durant l'exploitation du réseau s'effectue en rafraîchissant les états *Path* et *Resv*. Le rafraîchissement du *Path* s'effectue par le PLR et le *Resv* est rafraîchie par le MP en envoyant des messages *Resv* aux destinations IP contenues dans l'objet PHOP du message *Path* reçu via le tunnel de réserve.

3.4.7 Procédures à suivre pour calculer les chemins alternés

Pour établir les chemins alternés, on utilisera le protocole CSPF. Avant de calculer les chemins avec CSPF, il faut que le PLR collecte les informations suivantes :

- la liste des nœuds en aval (*downstream*) par lequel passe le LSP protégé ;
- les nœuds/liens en aval (*downstream*) que l'on veut éviter ;
- les liens unidirectionnels en amont (*upstream*) par lesquels passent les LSP ;
- les contraintes spécifiques à la classe de trafic à protéger ;
- les informations sur les ressources disponibles du LSP comme la largeur de bande ;
- les informations sur les ressources disponibles des autres LSP.

Lors de l'application de l'algorithme CSPF pour calculer un chemin alterné, les contraintes suivantes doivent être satisfaites :

- l'adresse source du LSP de réserve est l'adresse du PLR courant ;
- le LSP de réserve ne doit pas traverser les nœuds et les liens pour lesquels on veut assurer une protection ;
- le chemin de réserve doit satisfaire les contraintes de ressources du LSP protégé.

Si le calcul réussit, le PLR doit sauvegarder le résultat dans sa mémoire cache. Le chemin de réserve doit être aussi court que possible, et il doit se fusionner avec le LSP protégé au nœud MP, qui constitue la première intersection entre le LSP primaire et le LSP secondaire.

CSPF fonctionne de la manière suivante. D'abord, l'algorithme évalue tous les chemins possibles entre la source et la destination, i.e. entre les nœuds Ingress et Egress. Ces résultats sont conservés dans une liste. Ensuite, l'algorithme parcourt chaque route contenue dans la liste et vérifie si les contraintes (largeur de bande disponible, délai, nombre de nœuds, etc.) sont respectées. Si oui, alors ce chemin est placé dans une autre liste qui constitue l'ensemble des chemins possibles satisfaisant les contraintes. Une fois tous les chemins parcourus, l'algorithme CSPF implanté dans OPNET sélectionne au hasard un des chemins respectant les contraintes et le retourne lorsque la fonction **cspf_rte_compute** est appelée. Pour implanter notre approche, nous avons modifié l'algorithme CSPF de OPNET. Nous avons renommé cette fonction **cspf_rte_compute_list** avec les modifications suivantes :

1. D'abord, au lieu de retourner un seul chemin choisi aléatoirement, **cspf_rte_compute_list** retourne tous les chemins respectant les contraintes.
2. Lors de l'appel de la fonction, le chemin ayant le plus petit nombre de nœuds est retenu. Les autres chemins sont sauvegardés en mémoire comme chemins possibles en cas de panne. Ils peuvent être associés au même LSP ou à des LSP différents. Il faut noter que, dans le cas présent, les chemins dont il est question

constituent les différentes routes possibles que peut emprunter le LSP qui est un LSP dynamique. Les chemins sont conservés dans la variable **List* routes_lptr** d'un attribut de type **MplsT_Path_Info**. **MplsT_Path_Info** est une structure de données qui contient les attributs des LSP. La définition de la structure est illustrée à la Figure 3.4.

```
typedef struct {
    Objid   object_id;          /* Object ID of the path. Will be valid if the     */
                                /* if the path is present as an object in the      */
                                /* graphical user interface. Else the value is     */
                                /* OPC_OBJID_INVALID                               */

    char*   name;               /* Unique name identifying the path.               */

    void*   path_attrs;         /* Attributes of the path                          */

    List*   path_details_lptr;  /* Path details - contains the information         */
                                /* about the path configured by the user           */
    List*   hop_info_lptr;      /* Hop details - contains the actual hop info      */
    void*   path_state_ptr;     /* Any client specified state can be stored        */
    List*   routes_lptr;        /* List of diff routes that this path can take     */ }
MplsT_Path_Info;
```

Figure 3.4 Définition de la structure MplsT_Path_Info

Lors d'une panne sur le chemin principal du LSP, l'Ingress tentera de rerouter le LSP sur un des chemins contenus dans **routes_lptr**. C'est la fonction **rsvp_handle_failure()** qui est responsable de faire cet appel à la fonction **rsvp_start_lsp_switchover()**.

3. Si la route n'appartient pas au LSP, alors le trafic sera routé sur un autre LSP. L'Ingress tentera alors de rerouter le trafic sur ce LSP.
4. Finalement, s'il n'existe pas de LSP capable de supporter la charge de trafic, il faudra alors signaliser un nouvel LSP en utilisant les chemins disponibles dans routes_lptr. Cette situation ne sera pas implémentée, car on a une hypothèse de bi-connexité qui assurera la présence d'une route existante.

CHAPITRE IV
ÉVALUATION DE PERFORMANCE

Dans le chapitre précédent, nous avons décrit un algorithme de re-routage qui utilise les ressources existantes du réseau pour assurer la survivabilité. Cet algorithme se base sur les priorités de préemption plutôt que sur la réservation de ressources pour assurer la protection. De plus, la rapidité de la restauration est assurée par le fait que les chemins de protection alternés sont calculés à l'avance et sauvegardés en mémoire. Dans le présent chapitre, nous tenterons de confronter expérimentalement notre approche de survivabilité (PAR-UMTS) avec les deux approches existantes qui offrent les meilleures performances, soient la *Protection par Commutation (Protection Switching)* et le *Reroutage Rapide (Fast Reroute)*. Ces comparaisons expérimentales visent à déterminer les gains et les pertes de notre approche par rapport aux deux autres. Nous commençons ce chapitre en présentant les méthodes de *Reroutage Rapide* et de *Protection par Commutation* qui ont servi à notre évaluation de performance. Par la suite, nous élaborons le plan d'expérience, et finalement nous analysons les résultats.

4.1 Implémentation et prototypage du modèle

Comme mentionné au chapitre 2, les étapes critiques des mécanismes de *Reroutage Rapide* et de *Protection par Commutation* sont : la détection de pannes, la notification de la panne, et la commutation du trafic affecté par la panne sur un autre LSP préalablement réservé.

La détection de panne entraîne un changement de topologie (suppression de nœud ou de lien) qui est immédiatement détectée par OSPF. Les mécanismes de détection de pannes de MPLS détectent ce changement et font appel au mécanisme de notification pour aviser le PLR ou le routeur Ingress.

Lorsqu'une panne survient, elle doit être notifiée du point de détection au routeur de tête, de manière à ce que ce dernier puisse transférer le trafic du LSP actif au LSP de réserve. Pour ce faire, on utilise le message de notification *PathErr* dans RSVP-TE.

Sur réception du message de notification, le PLR ou l'Ingress commuteront le trafic sur le LSP de réserve déjà établi. Ce chemin peut être un *backup* (*Protection Switching*) ou un *bypass tunnel* (*Fast Reroute*).

Dans l'approche PAR-UMTS, le mécanisme de protection du trafic peut être enclenché soit par le routeur Ingress soit par le routeur PLR. L'approche PAR-UMTS peut être vue comme une extension du mécanisme de *Reroutage Rapide*, la seule différence étant que les chemins alternés (*Backups*) sont calculés avant la panne et ne sont pas réservés.

Les étapes critiques du mécanisme PAR-UMTS sont: le calcul de chemins alternés lors de l'établissement des LSP, la détection de pannes, la notification de la panne, et la commutation du trafic affecté par la panne sur un autre chemin alterné préalablement calculé.

Le calcul de chemins alternés

Le calcul des chemins alternés a lieu initialement lors de l'établissement des LSP pour router un trafic donné. L'algorithme CSPF a été étendu de manière à calculer plusieurs chemins possibles pouvant router le trafic. Ces chemins peuvent appartenir au même LSP ou à des LSP différents.

Si les chemins alternés calculés constituent des chemins différents pour router un LSP donné (LSPn), alors ils seront automatiquement utilisés lors d'une panne pour rerouter le LSPn. Donc, si le LSPn peut être routé par les chemins S1 et S2, et que S1 est choisi pour router le trafic initial, alors si S1 tombe en panne, le chemin S2 sera utilisé comme chemin alterné pour router le trafic. Il est sous-entendu que S1 et S2 satisfont les contraintes du trafic. Il n'est alors pas nécessaire de signaler un nouvel LSP, puisque le chemin S2 fait partie des chemins possibles de LSPn. Dans ce cas on aura :

$$S1 \in LSPn \text{ et } S2 \in LSPn.$$

Si les chemins alternés calculés ne peuvent faire partie du même LSP, alors on aura :

$$S1 \in LSP1 \text{ et } S2 \in LSP2, \text{ pour } LSP1 \neq LSP2$$

Si S1 subit une panne, alors pour router le trafic par S2, il faudra soit commuter le trafic de LSP1 à LSP2 si LSP2 existe ou signaliser LSP2 s'il n'existe pas.

La détection de pannes

La détection de panne entraîne un changement de topologie (panne de nœud ou de lien) qui est immédiatement détectée par OSPF. Les mécanismes de détection de pannes de MPLS détectent ce changement et font appel au mécanisme de notification pour aviser le PLR ou le routeur Ingress, comme c'est le cas pour la *Protection par Commutation* ou le *Reroutage Rapide.*

La notification de pannes

Lorsqu'une panne survient, elle doit être notifiée par le point de détection ou le routeur de tête, de manière à ce que ce dernier puisse transférer le trafic du LSP actif au LSP de réserve. Pour ce faire, le message de notification *PathErr* dans RSVP-TE est utilisé avec MPLS-TE. Dans le cas de notre implémentation, le message de notification sera envoyé au routeur Ingress.

La commutation du trafic

Sur réception du message de notification, le PLR ou l'Ingress commuteront le trafic sur le LSP alterné déjà calculé. S'il n'existe pas de LSP associé au chemin alterné calculé, alors l'Ingress signalisera un nouvel LSP qui sera routé par ce chemin.

4.2 Choix des métriques et modélisation des sources de trafic

Dans cette section, nous commencerons par élaborer les métriques utilisées pour l'évaluation de performance. Nous expliquerons ensuite comment nous avons modélisé les sources de trafic.

4.2.1 Choix des métriques

Nous utiliserons deux métriques comme base de comparaison dans notre évaluation de performance :

- le *temps de re-routage* : mesure la durée totale pour commuter le trafic d'un chemin à un autre ;
- le *délai de transmission* : mesure le délai de transmission sur les LSP. On veut, entre autres, mesurer l'impact d'un taux d'utilisation élevé sur le délai de transmission, donc sur la QoS.

Pour que les mesures prises soient significatives, il faut s'assurer que le modèle utilisé reflète le plus fidèlement possible la réalité. Les contraintes à respecter concernent :

- le modèle de trafic (i.e. la représentation des sources de trafic) ;
- la quantité de sources et le débit total sur les liaisons.

4.2.2 Modélisation des sources de trafic

Afin de réaliser le prototype, il faut modéliser les différents types de trafic représentant chaque classe, soit la voix ou vidéo-conférence HQ (*Conversational*), la vidéo-conférence LQ (*Interactive*), la vidéo sur demande (*Streaming*), et les trafics de données tels les courriers électroniques et les fichiers (*Background*).

Pour que la modélisation soit significative, il faut utiliser environ 15-25 sources pour chaque type de trafic. Deux options sont à considérer :

- utiliser 15-25 sources séparément ;
- utiliser une agrégation pour chaque type de trafic à l'aide de PDF approprié.

Dans notre implémentation, nous avons utilisé un total de 60 sources de voix. Deux LSP sont configurés pour la voix. Sur chaque LSP, on retrouve 15 nœuds source de voix et 15 nœuds de destination. Le type de trafic utilisé dans notre modèle est le G.729. Elle offre un débit de transmission de 8 Kbps, ce qui est en accord avec les spécifications

UMTS pour la classe conversationnelle (*Conversational*). Les caractéristiques du trafic sont données au Tableau 4.1.

Tableau 4.1 Caractéristiques du trafic de voix (Voix et Vidéo-conférence)

Paramètres	Valeurs
Nom	G.729
Tailles des trames (sec)	10 msec
Taux de codage (*Coding Rate*) (bits/sec)	8 Kbps
Classe de Service DiffServ (*Type of service*)	EF
Trames de voix par paquets	1

Le trafic de données a été représenté par un trafic de 128 Kbps, dont les caractéristiques sont données au Tableau 4.2.

Tableau 4.2 Caractéristiques du trafic de données

Paramètres	Valeurs
Protocole de Transport	UDP
Type de Service	Best Effort
Flot de données (*Data rate*)	128 Kbps

4.3 Plan d'expérience

Dans cette section, nous allons d'abord identifier les facteurs à mesurer lors des simulations. Ensuite, nous décrirons les tests effectués pour la validation du modèle.

4.3.1 Identifications des facteurs

Afin de valider le modèle, nous avons divisé les tests en sessions de simulation. L'objectif de ces sessions est de prendre des mesures en faisant varier les paramètres susceptibles d'influencer le comportement de l'algorithme. Les facteurs à mesurer sont le temps de reroutage et le délai de transmission, car ce sont ces facteurs qui vont servir à

comparer notre approche avec le mécanisme de *Protection par commutation*. Les facteurs variables seront le taux d'utilisation des liens et le nombre de nœuds entre le point de panne et le nœud Ingress. Ces deux facteurs sont pertinents pour les raisons suivantes :

- le taux d'utilisation des liens : Ce facteur induit des délais de transmission et de propagation qui peuvent faire varier le temps de notification et par conséquent le temps de reroutage. De plus, après que la commutation du trafic ait été enclenchée, un taux d'utilisation élevé peut faire varier le délai de transmission sur le chemin alterné, ce qui peut résulter en une dégradation de la qualité de service.
- le nombre de nœuds entre le point de panne et le nœud Ingress : Ce paramètre est important, car le temps de notification peut varier si le message de notification de panne doit parcourir 5 nœuds plutôt qu'un.

Le Tableau 4.3 représente les facteurs variables des simulations et leurs descriptions.

Tableau 4.3 Facteurs et niveaux choisis pour la simulation de PAR-UMTS

Facteurs		**Niveaux**	
Nom	**Symbole**	**Nom**	**Description**
Utilisation des liens du chemin alterné	U	Grand	80 %
		Moyen	60 %
		Faible	40 %
Distance entre le PLR et l'Ingress	D	Grand	5 noeuds
		Moyen	3 noeuds
		Faible	1 noeud

Afin d'observer l'influence des paramètres représentés au Tableau 4.3 sur le temps de reroutage et le délai de transmission, on effectuera les séries de tests suivants. D'abord, on considérera le facteur U constant (i.e. U = 50 %) et on fera varier le facteur D. Dans

un deuxième temps, on considérera le facteur D constant (D = 3 noeuds) et on variera le paramètre U.

Test 1: (U, D_1, D_2, D_3)

Test 2: (D, U_1, U_2, U_3)

À chaque variation, on mesurera les deux paramètres que sont le temps de reroutage et le délai de transmission. Il y aura donc 12 mesures dans notre simulation pour chacun des cas suivants :

1- un bris simple de nœud ou de lien sur un LSP pouvant être routé sur au moins deux chemins. Le taux d'utilisation des liens sera de 40 % sur les chemins primaire et alterné (Cas 1) ;
2- un bris simple de nœud ou de lien sur un LSP pouvant être routé par un seul chemin. Il existe un deuxième LSP appartenant à la même classe de trafic (Cas 2) ;
3- un bris simple de nœud ou de lien sur un LSP pouvant être routé par un seul chemin. Il n'existe pas un deuxième LSP appartenant à la même classe de trafic, mais un LSP appartenant à une classe de trafic inférieure (Cas 3).

Au cours des simulations, nous avons considéré que le trafic du réseau est stable à l'intérieur de l'intervalle ΔT des simulations. Dans chaque cas, nous avons comparé les paramètres suivants : le temps de reroutage et le délai. Il est important de mentionné que plusieurs simulations ont été effectuées, mais que les résultats présentés dans cette section correspondent aux situations de pire cas. Cette décision a été prise afin d'alléger le texte.

4.3.2 Tests sur le trafic de voix vidéo-conférence (*Classe conversationnelle UMTS*)

Les réseaux utilisés pour effectuer la simulation sont représentés aux figures 4.1 et 4.2. La Figure 4.1 illustre la *Protection par Commutation*. Le LSP1 sert à router le trafic de voix en provenance du nœud node_0, et le LSP2 est réservé comme chemin de réserve (*Backup*). On est en présence de la *Protection 1 : 1*.

Chemin primaire : **LSP1** = {Ingress, LSR_1, LSR_5, LSR_7, Egress}

Chemin de réserve: **LSP2** = {Ingress, LSR_3, LSR_8, Egress}

À la Figure 4.2, on remarque d'abord la présence de trois LSP. Les LSP ont les caractéristiques suivantes :

LSP1 = {Ingress, LSR_1, LSR_5, LSR_7, Egress} OU {Ingress, LSR_1, LSR_6, LSR_7, Egress}

LSP2 = {Ingress, LSR_3, LSR_8, Egress}

LSP3 = {Ingress, LSR_4, LSR_10, LSR_11, LSR_12, Egress}

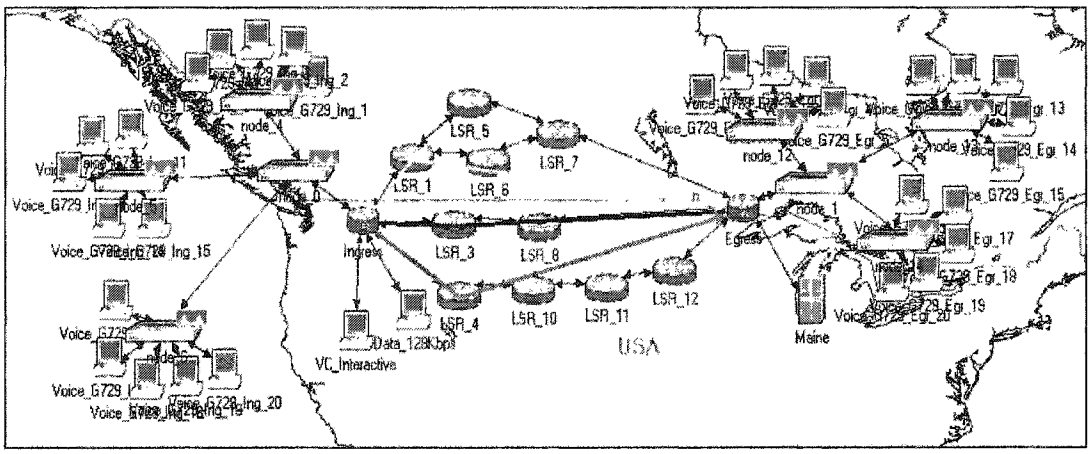

Figure 4.1 Réseau simulé avec trafic de voix (*Protection par Commutation*)

Les liens utilisés sur le réseau dorsal sont des DS1 (1.544 Mbps), et ceux du réseau d'accès sont des DS0 (64 Kbps). La durée d'une simulation est de 600 secondes.

Pour les quatre séries de tests suivantes, on évalue l'impact d'une charge réseau (sur le chemin alterné) de 40 %, 60 % et 80 % sur le temps de reroutage et le délai de transmission. La distance entre l'Ingress et le point de panne reste constante.

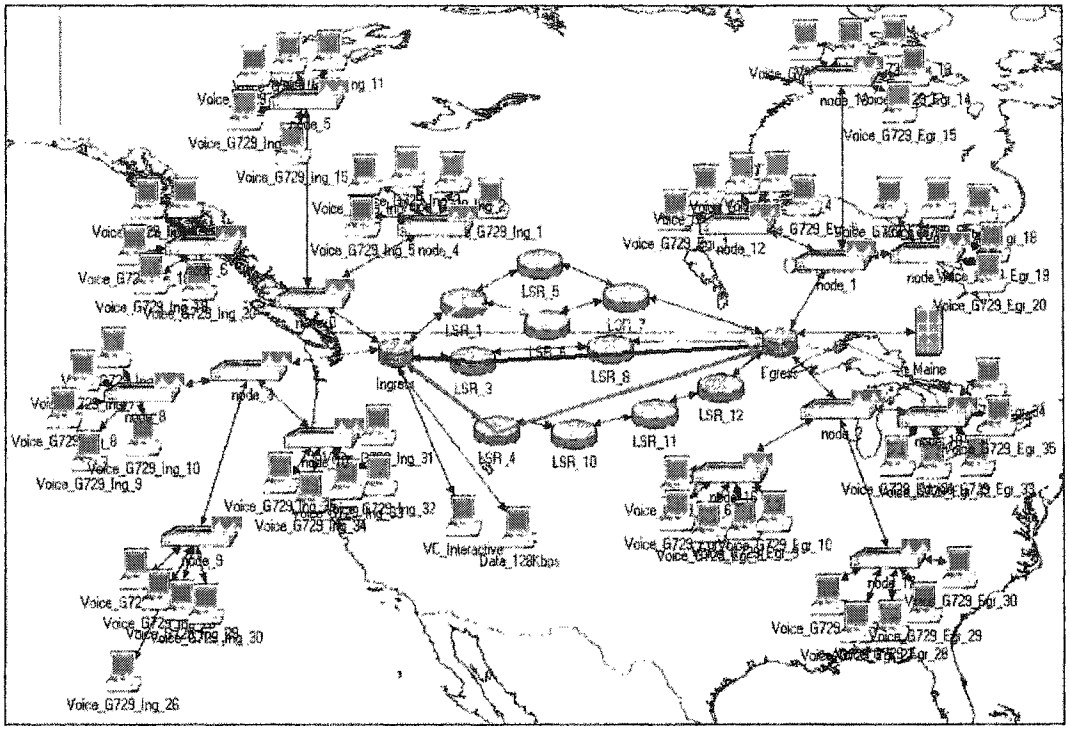

Figure 4.2 Réseau simulé avec trafic de voix (*PAR-UMTS*)

Les tests suivants sont effectués afin de valider le modèle :

Test 1

On effectue un essai en utilisant la *Protection par Commutation*. Le LSR_1 tombe en panne au temps t = 400 secondes. Le taux d'utilisation des liens sera de 40 % sur les chemins primaire et alterné.

Test 2

Le trafic provenant du nœud *node_0* est routé sur le LSP1 et le trafic provenant du nœud *node_3* est routé sur LSP2. Le LSR_5 tombe en panne au temps t = 400 secondes. Le taux d'utilisation des liens sera de 40 % sur les chemins primaire et alterné (Cas 1).

Test 3

Le trafic provenant du nœud *node_0* est routé sur le LSP1 et le trafic provenant du nœud *node_3* est routé sur LSP2. Le LSR_1 tombe en panne au temps t = 400 secondes. Le taux d'utilisation des liens sera de 30 % sur le chemin primaire et passera à 40 %, 60 %, et 80 % sur les chemins alternés. Ces augmentations correspondent à la situation où on

commute le trafic du chemin primaire sur un chemin alterné contenant déjà du trafic (Cas 2).

Test 4

Le trafic routé sur le LSP1 est de la voix et le trafic routé sur le LSP2, du trafic de données. LSP1 peut être routé par un seul chemin, le chemin alterné se trouvant sur LSP2, car il emprunte un chemin plus court que le LSP3. Le taux d'utilisation des liens sera de 30 % sur le chemin primaire et passera à 40 %, 60 %, et 80 % sur les chemins alternés. Ces augmentations correspondent à la situation où on commute le trafic du chemin primaire sur un chemin alterné contenant déjà du trafic (Cas 3).

4.4 Analyse des résultats

Nous analyserons successivement les résultats obtenus par les mécanismes de *Protection par Commutation* et PAR-UMTS. Commençons d'abord par les résultats des tests pour la voix et la video-conférence, et étudions l'impact de la charge réseau sur le temps de reroutage et le délai de transmission.

Test 1

On remarque que lorsque le LSR_1 du chemin S1 tombe en panne, le trafic est transmis sur le chemin S2. Le chemin S2 est réservé uniquement à la protection du chemin S1. Le temps de commutation du chemin S1 au chemin S2 est de 4.9 msec, ce qui est nettement inférieur au 50 msec requis pour la voix. De plus, le délai de transmission, représenté à la Figure 4.3, reste stable et faible (10.5 msec), ce qui permet d'affirmer que les pertes de paquets sont très faibles.

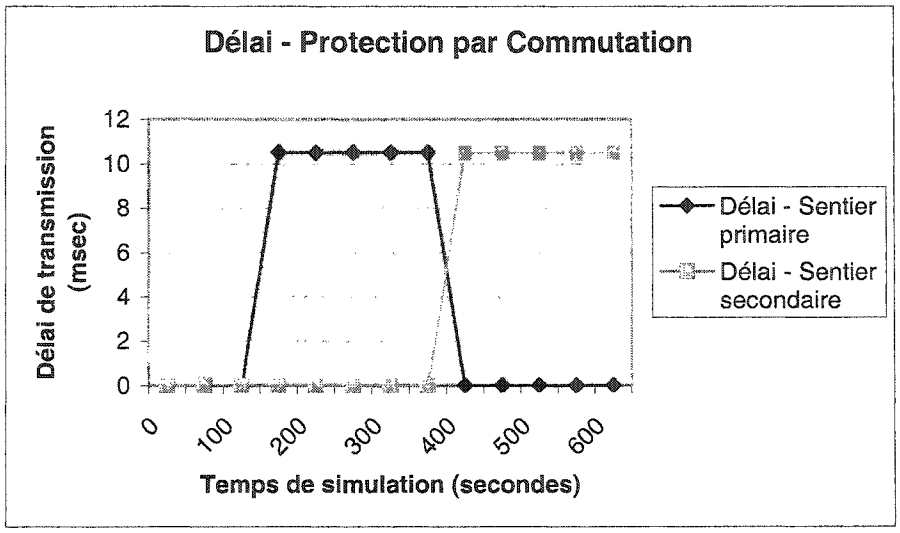

Figure 4.3 Délai de transmission (*Protection par Commutation*)

Avec l'algorithme PAR-UMTS, on obtient les résultats suivants :

Test 2

Lorsque le LSR_5 tombe en panne (chemin S1), le trafic est transmis sur le LSR_6 (chemin S2). Comme les chemins S1 et S2 sont deux routes possibles pour le LSP1, alors le trafic continue à être transmis sur ce LSP. À la Figure 4.4, on voit que le temps de commutation du chemin S1 au chemin S2 est de 3.6 msec, ce qui est nettement inférieur au 50 msec requis pour la voix et représente une amélioration de 26.53 % par rapport aux performances de la *Protection par Commutation* implémentée dans OPNET. De plus, le délai de transmission, représenté à la Figure 4.5, reste stable et faible (10.5 msec), ce qui permet d'affirmer que les pertes de paquets sont très faibles.

Le gain dans cette situation se trouve au niveau des opportunités d'affaire. Dans le cas de la *Protection par Commutation*, il faut réserver un LSP contenant deux routeurs intermédiaires et un lien DS3 uniquement pour la protection. Avec PAR-UMTS, on peut utiliser ces ressources pour offrir des services générant des revenus.

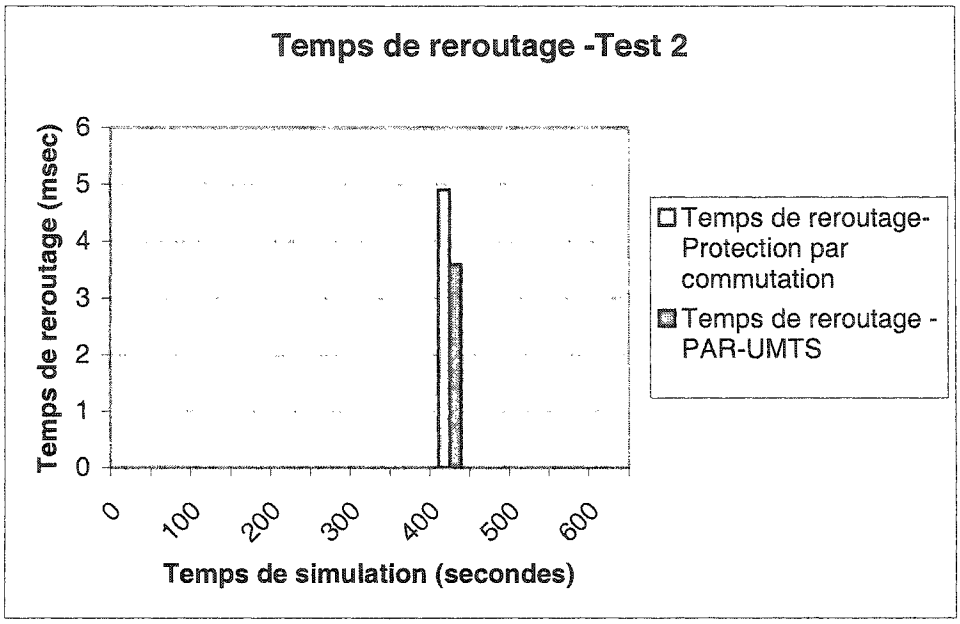

Figure 4.4 Temps de reroutage (*Test 2*)

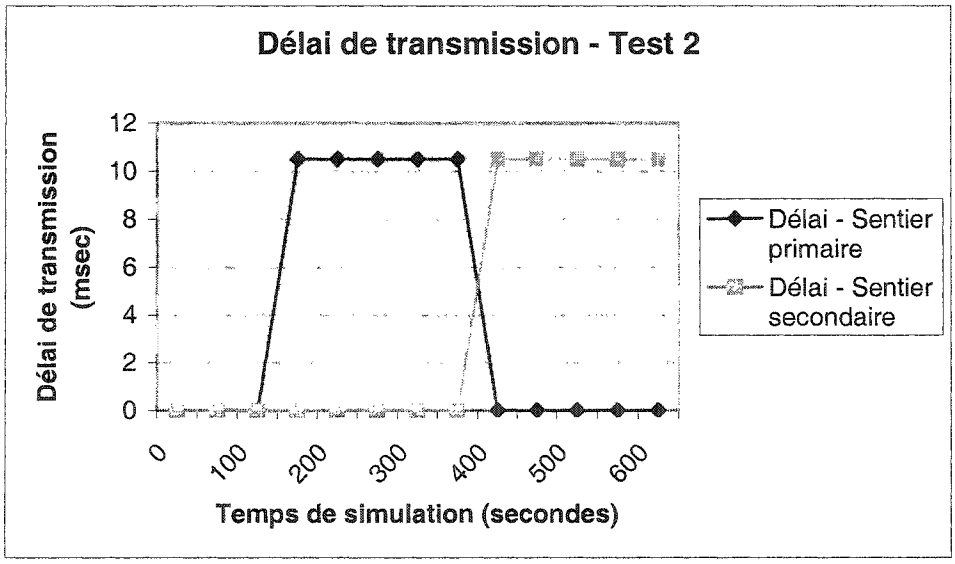

Figure 4.5 Délai de transmission (*PAR-UMTS – Test 2*)

Test 3

Comme les chemins S1 et S2 appartiennent à deux LSP différents, alors le nœud Ingress doit commuter le trafic. Le temps de commutation du chemin S1 au chemin S2

est représenté à la Figure 4.6 et est de 3.6 msec. Ce résultat est comparable au résultat précédent où les chemins S1 et S2 appartenaient au même LSP. Cette similitude s'explique par le fait que les chemins alternés S2 (des tests 1.2 et 1.3) se trouvent à la même place en mémoire et ils existent déjà. Donc, dans les deux cas, l'Ingress n'a qu'à lire sa table et commuter le trafic de S1 à S2.

Par contre, on constate une différence au niveau du délai de transmission illustré à la Figure 4.7. Lors de la commutation du trafic du chemin primaire au chemin alterné, le délai de transmission passe de 10.5 msec à 29 msec à 48 msec respectivement pour des charges réseau de 40 %, 60 % et 80 %. Cette augmentation s'explique par l'augmentation de trafic sur le chemin alterné. Si on considère qu'un appel interurbain doit traverser environ 7 domaines administratifs et un total de 30 routeurs (Pan, 2002), et que le délai de bout en bout doit être inférieur à 150 msec, alors le délai par domaine doit être d'environ 21.4 msec. Maintenant, il est à noter que le délai sans panne est d'environ 10.5 msec par domaine, ce qui donne un délai de 73.5 msec de bout en bout.

Lors de l'évaluation du délai de bout en bout, nous avons négligé le délai de transmission entre l'unité mobile et le routeur d'accès au réseau dorsal IP/MPLS. Nous considérons le délai de bout en bout comme étant le délai de transmission à l'intérieur du réseau dorsal pour les raisons suivantes. D'abord, les liens de transmission sur le réseau d'accès sont généralement pourvus de grandes capacités (bits/secondes) permettant un accès instantané au réseau dorsal. De plus, la distance géographique que doivent parcourir les données sur le réseau d'accès est négligeable par rapport à la distance à parcourir sur le réseau dorsal, puisque celui-ci s'étend sur des centaines, voir des milliers de kilomètres. Finalement, le niveau de congestion sur le réseau dorsal est nettement plus élevé que celui du réseau d'accès, car le réseau dorsal doit supporter des trafics provenant de plusieurs réseaux d'accès différents.

Lors d'une panne sur un domaine, si dans le pire cas (Taux d'utilisation = 80 %) le délai monte à 48 msec, alors le délai de bout en bout sera égal à (6 x 10.5 + 1 x 48 = 111) 111 msec s'il y a une panne seulement et (5 x 10.5 + 2 x 48 = 148.5) 148.5 msec dans le cas de deux pannes simultanées. Ce délai monte à 186 msec s'il y a une panne sur

trois domaines simultanément. Il faut donc 3 pannes simultanées pour dépasser un délai de bout en bout de 150 msec. La probabilité d'avoir 3 pannes simultanément étant très faible, voire proche de zéro, on peut donc considérer que le délai observé est acceptable. La probabilité d'avoir une panne sur trois domaines simultanément est évaluée à 5.7×10^{-9} %. Nous allons maintenant expliquer les hypothèses émises ainsi que les détails du calcul.

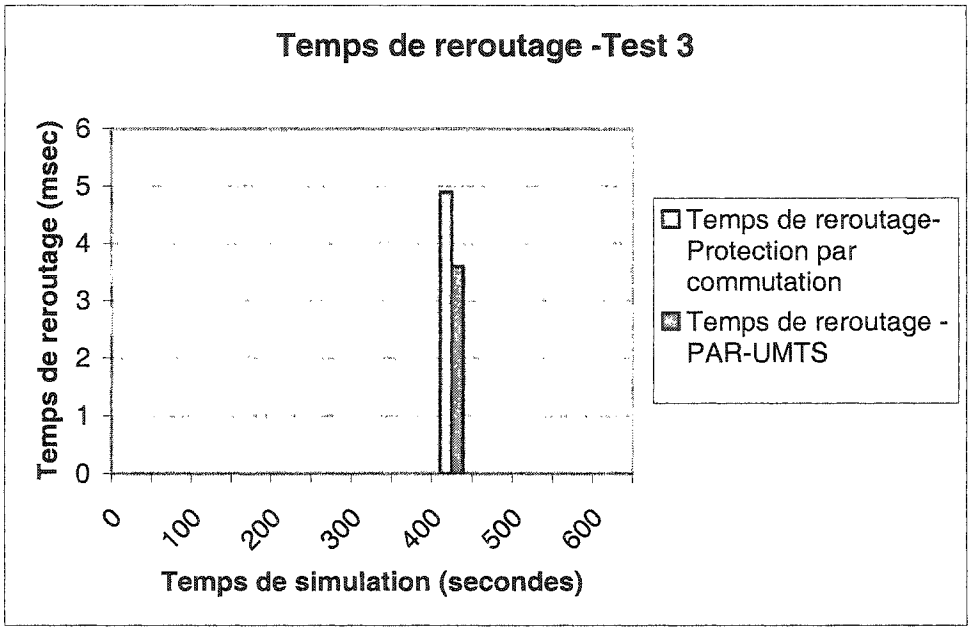

Figure 4.6 Temps de reroutage (*Test3*)

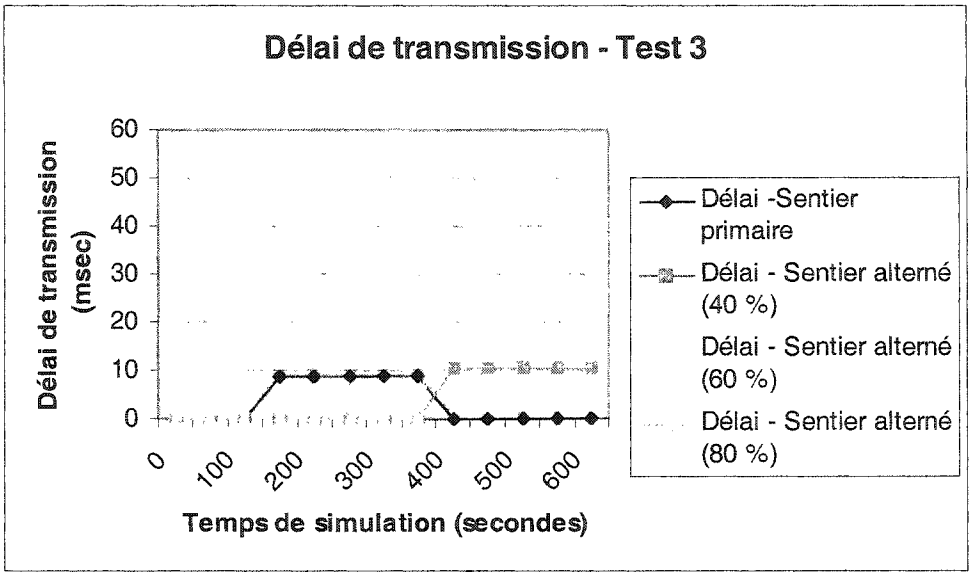

Figure 4.7 Délai de transmission (*PAR-UMTS – Test 3*)

Hypothèses :

1. Étant donné l'hypothèse de bi-connexité des liens énoncés précédemment, on est assuré qu'il y aura toujours un chemin disponible suite à une première panne pour le trafic conversationnel ;
2. On suppose une indépendance de pannes de nœuds entres-elles ;
3. On suppose une indépendance des pannes de LSP ;
4. On suppose aussi une non-corrélation entre les pannes de plusieurs domaines distincts. D'un point de vue probabiliste, s'il y a une panne sur n domaines simultanément, alors ces n pannes sont considérés comme des événements indépendants ;
5. En se basant sur les spécifications émises par les manufacturiers CISCO et JUNIPER, le taux de disponibilité des équipements de réseaux (Routeurs et Commutateurs) est de 99.999 %. Ce taux de disponibilité est calculé avec la relation : A = [MTBF/(MTBF + MTTR)]. Nous sommes donc en présence d'un *Carrier Class Grade Voice Services*.

6. La panne sur un domaine sera dû uniquement à une panne de nœud (Routeur ou Commutateur). La panne de lien sera négligée, car les liens sont en fibre optique. Avec la fibre optique, il est pratiquement impossible d'établir une probabilité de défaillance (ou de disponibilité) pour une panne causée par un élément extérieur tels un déni de service ou un bris dû à une coupure de câble.

Soient A la disponibilité des composants du réseau (Routeurs et Commutateurs) et U_e la probabilité qu'un composant du réseau tombe en panne. De plus, soit trois événements a, b, et c. Si a et b sont indépendants, la probabilité :

$P(a \cap b) = P(a) * P(b)$. De même, si a, b et c sont indépendants, alors on aura :

$P(a \cap b \cap c) = P((a \cap b) \cap c) = P(a \cap b) * P(c) = P(a) * P(b) * P(c)$

Détails de calcul

La relation entre A et U_e est donnée par : $A = 1\text{-}U_e$, où $A = 0.99999$ et $U_e = 1x10^{-5}$. Si on considère un LSP comportant 4 nœuds, la probabilité que ce LSP tombe en panne est donnée par :

$P_L =$ P(Nœud 1 tombe en panne) * P(Les trois autres nœuds restent disponibles)
+ P(Nœud 2 tombe en panne) * P(Les trois autres nœuds restent disponibles)
+ P(Nœud 3 tombe en panne) * P(Les trois autres nœuds restent disponibles)
+ P(Nœud 4 tombe en panne) * P(Les trois autres nœuds restent disponibles)

$P_L = 4* U_e A^3 = 4 * (1x10^{-5})*(0.99999)^3 = 4x10^{-5} = 0.004\ \%$

Si un domaine possède trois LSP en moyenne, tel qu'illustré à la Figure 4.2, alors la probabilité d'avoir une panne sur un domaine est donnée par :

$P_D =$ P(LSP 1 tombe en panne) * P(Les deux autres LSP sont disponibles)
+ P(LSP 2 tombe en panne) * P(Les deux autres LSP sont disponibles)
+ P(LSP 3 tombe en panne) * P(Les deux autres LSP sont disponibles)

$P_D = 3* P_L (1- P_L)^2 = 3 * (4x10^{-5}) * (1- 4x10^{-5})^2 = 1.2x10^{-4} = 0.012\ \%$

En considérant qu'un réseau compte 7 domaines (Pan, 2002), alors la probabilité d'avoir deux pannes simultanées sur deux domaines distincts (toutes classes de trafic confondues) est donnée par :

P_{2D} = P(Domaine 1 en panne)* P(Domaine 2 en panne) * P(Les 5 autres domaine n'ont pas de panne) +
P(Domaine 1 en panne)* P(Domaine 3 en panne) * P(Les 5 autres domaine n'ont pas de panne)
+
P(Domaine 1 en panne)* P(Domaine 4 en panne) * P(Les 5 autres domaine n'ont pas de panne)
+
P(Domaine 1 en panne)* P(Domaine 5 en panne) * P(Les 5 autres domaine n'ont pas de panne)
+
P(Domaine 1 en panne)* P(Domaine 6 en panne) * P(Les 5 autres domaine n'ont pas de panne)
+
P(Domaine 1 en panne)* P(Domaine 7 en panne) * P(Les 5 autres domaine n'ont pas de panne)
+
P(Domaine 2 en panne)* P(Domaine 3 en panne) * P(Les 5 autres domaine n'ont pas de panne)
+
...

Donc, on aura:

$$P_{2D} = \sum_{i=1}^{6} \sum_{j=i+1}^{7} P_i * P_j * [(1 - P_D)^5], \qquad \text{avec } P_i = P_j = P_D$$

$$P_{2D} = \sum_{i=1}^{6} \sum_{j=i+1}^{7} P_D^2 [(1 - P_D)^5]$$

Le nombre de possibilités de pannes simultanées sur deux domaines est représenté au Tableau 4.4.

Tableau 4.4 Possibilités de pannes simultanées sur 2 domaines

Possibilités de pannes sur deux domaines simultanément (i, j)					
(1, 2)	(2, 3)	(3, 4)	(4, 5)	(5, 6)	(6, 7)
(1, 3)	(2, 4)	(3, 5)	(4, 6)	(5, 7)	
(1, 4)	(2, 5)	(3, 6)	(4, 7)		
(1, 5)	(2, 6)	(3, 7)			
(1, 6)	(2, 7)				
(1, 7)					

On voit à l'aide du Tableau 4.3 qu'il existe 21 possibilités. Donc, la valeur de P_{2D} sera :

$$P_{2D} = (6 * P_D^2 (1 - P_D)^5) + (5 * P_D^2 (1 - P_D)^5) + (4 * P_D^2 (1 - P_D)^5) +$$

$$(3 * P_D^2 (1 - P_D)^5) + (2 * P_D^2 (1 - P_D)^5) + (1 * P_D^2 (1 - P_D)^5)$$

$$P_{2D} = 21 * (P_D^2 (1 - P_D)^5) = 21 * (1.2\text{x}10^{-4})^2 * (1 - 1.2\text{x}10^{-4})^5$$

$$P_{2D} = 3.02\text{x}10^{-7} = 3.02\text{x}10^{-5}\ \% = 0.0000302\ \%$$

On voit par ce calcul que la probabilité d'avoir une panne sur deux domaines simultanément est très faible. Comparativement à la probabilité d'avoir une panne sur un LSP (0.012 %), on a 398 fois moins de chance d'avoir deux pannes simultanées que d'en avoir une. Donc, les résultats obtenus dans le cadre du Test 3 sont satisfaisants et nous pouvons conclure que l'algorithme se comporte bien.

La probabilité d'avoir une panne sur trois domaines simultanément est donnée par:

$$P_{3D} = \sum_{i=1}^{5} \sum_{j=i+1}^{6} \sum_{k=i+2}^{7} P_i * P_j * P_k * [(1 - P_D)^4], \qquad \text{avec } P_i = P_j = P_k = P_D$$

$$P_{3D} = \sum_{i=1}^{5} \sum_{j=i+1}^{6} \sum_{k=i+2}^{7} P_D^3 * [(1 - P_D)^4], \qquad \text{avec } P_i = P_j = P_k = P_D$$

Dans ce cas, les possibilités sont dénombrées au Tableau 4.5.

Tableau 4.5 Possibilités de pannes simultanées sur 3 domaines

Possibilités de pannes sur trois domaines simultanément (i, j, k)			
(1, 2, 3)	(1, 3, 4)	(1, 4, 5)	(1, 5, 6)
(1, 2, 4)	(1, 3, 5)	(1, 4, 6)	(1, 5, 7)
(1, 2, 5)	(1, 3, 6)	(1, 4, 7)	
(1, 2, 6)	(1, 3, 7)		
(1, 2, 7)			
(2, 3, 4)	(2, 4, 5)	(2, 5, 6)	
(2, 3, 5)	(2, 4, 6)	(2, 5, 7)	
(2, 3, 6)	(2, 4, 7)		
(2, 3, 7)			
(3, 4, 5)	(3, 5, 6)	(3, 6, 7)	
(3, 4, 6)	(3, 5, 7)		
(3, 4, 7)			
(4, 5, 6)	(4, 6, 7)		
(4, 5, 7)			
(5, 6, 7)			

On voit à l'aide du Tableau 4.5 qu'il existe 33 possibilités. Donc, la valeur de P_{3D} sera :

$$P_{3D} = 33 * P_D^3 * [(1 - P_D)^4] = 33 * (1.2 \times 10^{-4})^3 * (1 - 1.2 \times 10^{-4})^4$$

$$P_{3D} = 5.7 \times 10^{-11} = 5.7 \times 10^{-9} \%$$

Par ce calcul, on voit que la probabilité de panne sur trois domaines simultanément est proche de zéro (5.7×10^{-9} % ou 0.0000000057 %). Donc, la possibilité d'obtenir une panne sur quatre domaines simultanément est à toute fin pratique négligeable.

Le gain dans cette situation se trouve au niveau des opportunités d'affaire. Dans le cas de la *Protection par Commutation*, il faut réserver un LSP contenant deux routeurs intermédiaires et un lien DS3 uniquement pour la protection. Avec PAR-UMTS, on peut utiliser ces ressources pour offrir des services générant des revenus.

Test 4

On remarque à la Figure 4.8 que le temps de commutation du chemin S1 au chemin S2 est de 3.6 msec, ce qui est comparable au résultat précédent où les chemins S1 et S2 appartenaient au même LSP. Cette similitude s'explique par le fait que les chemins

alternés S2 (des Tests 2 et 3) se trouvent à la même place en mémoire et ils existent déjà. Donc, dans les deux cas, l'Ingress n'a qu'à lire sa table et commuter le trafic de S1 à S2.

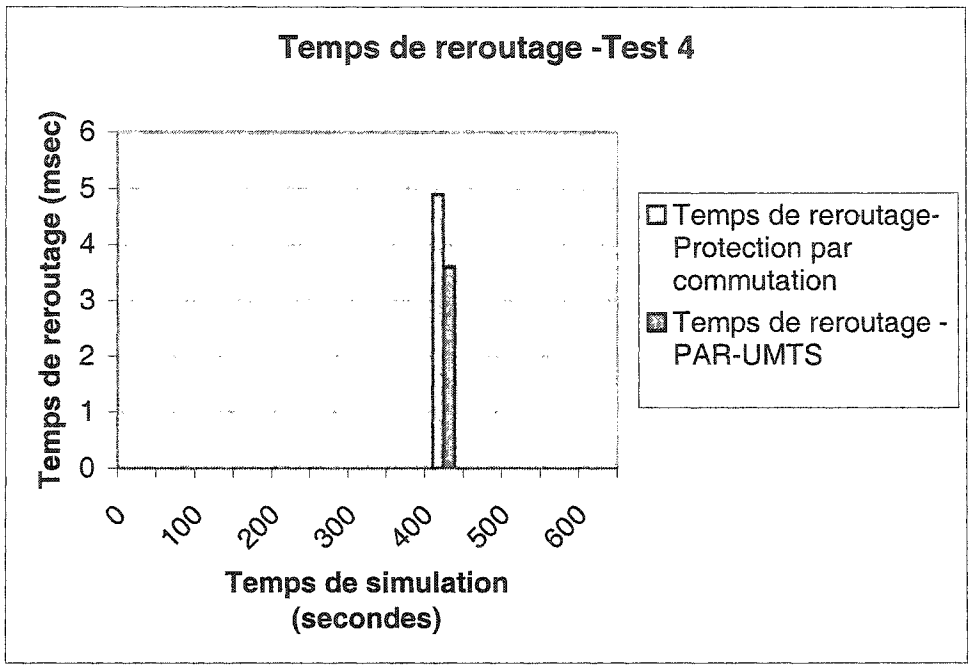

Figure 4.8 Temps de reroutage (*Test 4*)

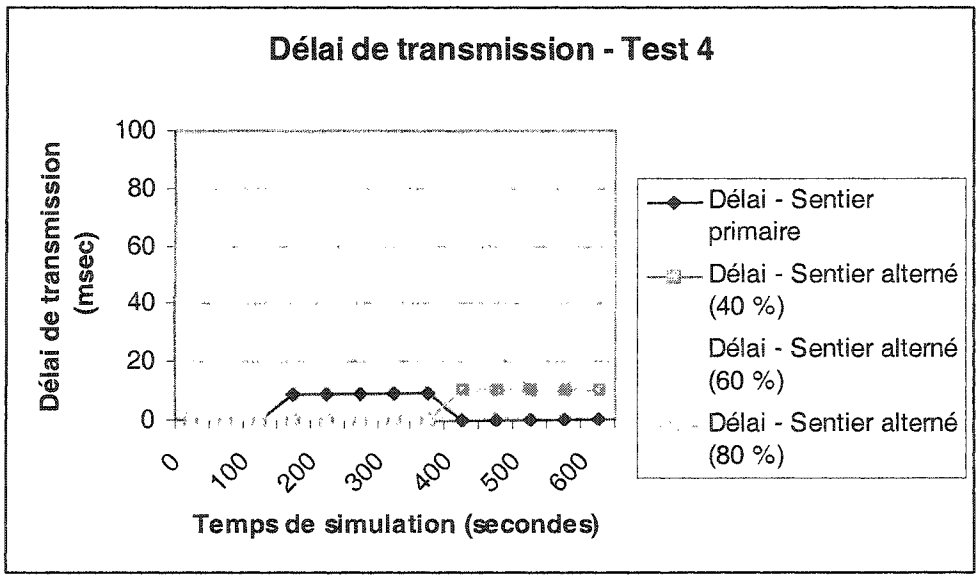

Figure 4.9 Délai de transmission (*PAR-UMTS – Test 4*)

Par contre, on constate une différence au niveau du délai de transmission. Lors de la commutation du trafic du chemin primaire au chemin secondaire, le délai de transmission passe de 10.5 msec à 65 msec dans le pire cas (Taux d'utilisation = 80 %). De plus, lors de la commutation, la voix est transférée sur un LSP qui contient des propriétés inférieures. Le délai bout en bout sur les sept domaines administratifs serait de (6 x 10.5 + 1 x 65 = 128) 128 msec. On observe un délai de bout en bout de 182 msec (> 150 msec) si la situation se produit sur deux domaines simultanément (avec une probabilité de 3.02 x 10^{-5} %).

Les résultats du test 4 font ressortir le fait que la commutation du trafic conversationnel sur un LSP de classe inférieure est coûteuse en terme de délai de transmission. Mais la probabilité d'atteindre un état critique est très faible, voire même quasi-nulle. Si le délai peut sembler élevé sur un domaine, il devient tout à fait acceptable dans l'optique globale d'un délai de bout en bout.

En résumé, les performances de cette approche sont excellentes, comparativement aux méthodes standards. D'abord, notre approche offre un temps de réponse similaire aux mécanismes de *Protection par Commutation* et de *Reroutage Rapide*. Par contre, elle a l'avantage de ne pas réserver de ressources, donc elle optimise l'utilisation de réseau. Par rapport aux mécanismes de chemins alternés, notre approche offre le même type de performance au niveau de l'optimisation des ressources, mais elle s'avère plus rapide au niveau du temps de réponse.

4.5 Discussion et améliorations

Afin d'optimiser les résultats et les performances de l'algorithme, plusieurs éléments peuvent être améliorés.

Modélisation avec trafics et équipements UMTS

Afin de modéliser le trafic conversationnel UMTS, nous avons utilisé des générateurs utilisant la voix à 8 Kbps. La raison est que nous ne disposions pas de la

licence UMTS en laboratoire. Il serait intéressant dans des travaux futurs d'intégrer la licence UMTS à la licence MPLS de OPNET de manière à simuler le trafic en accès avec des terminaux UMTS, tout en conservant un réseau dorsal IP/MPLS.

Tester plus de cas

Afin de simplifier les tests, nous avons émis une série d'hypothèses simplificatrices. D'abord, les tests se sont limités au trafic des classes *Conversationnel* et *Background* de UMTS. Même si intuitivement nous sommes portés à croire que le comportement de l'algorithme serait identique pour les classes *Streaming* et *Interactive*, il serait intéressant de répéter les tests pour ces classes de trafic.

De plus, dans l'implémentation de l'algorithme, nous avons considéré uniquement les cas où les LSP étaient déjà signalisés. Donc, les chemins alternés calculés pour la restauration appartiennent à des LSP déjà établis. Une amélioration possible au modèle PAR-UMTS serait de considérer le cas où les chemins existent, mais que le LSP utilisant le chemin n'est pas encore signalisé. Il faudrait alors ajouter des mécanismes de signalisations dynamiques de LSP afin de signaliser de nouveau LSP avec les contraintes appropriées

Finalement, nous avons considéré le cas d'une protection globale du trafic entre l'Ingress et l'Egress. Ce cas constitue une borne supérieure (Temps de reroutage et délai de transmission). Une amélioration à ces travaux serait de tester le cas de la protection locale en ajoutant les fonctionnalités de l'Ingress à des routeurs intermédiaires.

Réglages et ajustements

Présentement, l'implémentation dans OPNET des mécanismes de protection (*Protection par Commutation* et *Reroutage Rapide*) et de restauration ne renvoie pas le trafic sur le chemin primaire après que celui-ci a été réparé. C'est que, lors d'une faute, le trafic est commuté sur un autre chemin. Par contre, une fois que le chemin primaire a été réparé, le trafic continue de circuler sur le chemin alterné (ou de réserve) au lieu de retourner sur le chemin primaire rétabli. Ce comportement est dû au fait que, lors de la

commutation du trafic, les références au LSP primaire sont effacées. Il serait intéressant dans ce cas d'implémenter un mécanisme qui permettrait de réutiliser un LSP primaire une fois qu'il est réparé.

Une manière de minimiser des délais de transmission qui avoisine les 48 msec dans certains cas serait de modifier le *Buffer* (Queue).

CHAPITRE V
CONCLUSION

5.1 Synthèse des travaux

Le problème que nous avons abordé dans ce mémoire est un problème ouvert qui peut être résolu avec plusieurs approches. Nous avons proposé un nouvel algorithme de survivabilité qui est une extension de deux approches opposées. D'une part, elle utilise le même mécanisme que le *Routage Alterné* pour calculer des chemins de réserve (alternés), mais elle calcule ces chemins avant la panne, ce qui fait que les chemins alternés sont connus d'avance, sans être réservés. L'algorithme permet d'autre part d'assurer un temps de reroutage rapide sans avoir à réserver des ressources.

L'algorithme a été implémenté sur OPNET Modeler afin d'en évaluer la performance. Il s'agissait donc d'implémenter l'algorithme, pour ensuite comparer ses performances avec la *Protection par Commutation*. Le modèle est constitué d'une série de chemins (LSP) appartenant chacun à une classe de trafic UMTS prédéfinie. Chaque chemin est constitué de 3 à 4 nœuds. L'algorithme a été implémenté dans le routeur de tête (*Ingress*). Une analyse de performance nous a permis de définir les indices de performance du modèle. Après l'identification de ces indices, nous avons réalisé des mesures qui ont permis de conclure que l'approche PAR-UMTS est plus adaptée à nos objectifs. En effet, les mesures montrent que la *Protection par Commutation* est plus coûteuse en termes de ressources, car il faut réserver les chemins de protection. En ce qui a trait au modèle PAR-UMTS, il offre des temps de restauration comparable à la *Protection par Commutation*, mais a l'avantage d'être plus économique sur l'utilisation des ressources, car il n'y a pas de réservation. L'approche PAR-UMTS utilise les ressources existantes sur le réseau pour établir des chemins alternés qui pourront être utilisés en cas de panne.

L'algorithme présente les avantages suivants :

- il est conçu pour optimiser les ressources du réseau (les capacités des liaisons et les équipements) ;
- il est rapide car les chemins alternés sont calculés avant la panne ;
- il est simple d'implémentation, puisque la majeure partie de son architecture se base sur les mécanismes de gestion de fautes existant dans MPLS. De plus, dans l'implémentation présentée dans ce mémoire, c'est le routeur de tête (Ingress) qui se charge de la restauration.

Les fonctionnalités de l'algorithme sont extensibles. D'abord, on peut étendre les fonctions du routeur de tête à des routeurs intermédiaires. Ensuite, on peut étendre l'algorithme pour qu'il puisse protéger d'autres types de trafic que le trafic UMTS. Cependant, bien que l'algorithme PAR-UMTS apparaisse comme le meilleur, cette solution n'est pas parfaite et peut bénéficier de quelques améliorations.

5.2 Limitation des travaux

La survivabilité du trafic est un problème qui présente plusieurs facettes. Dans ce mémoire, nous avons émis plusieurs hypothèses. Une des hypothèses émises lors de l'implémentation était que la réservation des ressources se fait de manière statique et que le flot de trafic demeure constant sur un intervalle de temps déterminé qui correspondait au temps de simulation. Or, dans la réalité, le flot de trafic varie pour chaque classe de trafic puisque la quantité d'usagers sur le réseau est dynamique. Une amélioration possible serait d'ajouter de la signalisation qui permettrait une mise à jour dynamique des tables de routage de chemins alternés suivant la variation de disponibilité du réseau. Trois approches peuvent être envisagées. D'abord, la mise à jour peut se faire à chaque fois qu'un usager se connecte sur le réseau. Cette approche a l'avantage d'offrir une table de reroutage qui reflète parfaitement l'état de réseau. Par contre, elle a l'inconvénient de nécessiter un grand nombre de messages de signalisation, ce qui risque de diminuer les performances du réseau en créant de la congestion. Une autre approche serait de faire la mise à jour par intervalles de temps régulier. Le défi de cette méthode est de choisir des intervalles assez courts qui permettent d'avoir une table de routage qui

reflète le plus possible la réalité du réseau, mais assez longue pour diminuer le nombre de messages de signalisation sur le réseau. La troisième approche qui, selon nous, offre le meilleur compromis, serait d'établir des seuils de variation sur les liens. La mise à jour des tables de routage alternés aurait lieu lorsque ces seuils sont atteints. Par exemple, si un chemin alterné a été établi et que la somme des trafics de ce chemin et du chemin qu'il protège équivaut à une utilisation de 65 %, et que les performances peuvent être maintenues jusqu'à une utilisation de 80 %, alors on peut établir le seuil de variation à 15 %. Si la somme des deux trafics varie de plus de 15 %, il y aura une mise à jour de la table.

Une autre hypothèse émise durant l'implémentation est la bi-connexité des LSP. Cette hypothèse garantissait l'existence de LSP alternés en cas de panne. Par contre, on pourrait supposer qu'il existe des ressources sur le réseau, mais que ces ressources ne soient pas assignées à un LSP particulier. L'amélioration qui peut être apportée à notre algorithme serait d'ajouter de la signalisation permettant d'établir de nouveaux LSP pour une classe de trafic déterminée de façon dynamique. Cela offrirait une option supplémentaire aux options proposées.

5.3 Orientations de recherche future

Plusieurs améliorations peuvent être apportées au modèle proposé et plusieurs de ces améliorations peuvent faire l'objet de sujets de recherche. Dans l'approche proposée, on considère uniquement le cas où tous les chemins alternés sont déjà établis et opérationnels. Par contre, dans la pratique, il se pourrait qu'on ait besoin de signaliser un nouvel LSP après une panne. Donc, une amélioration possible serait de mettre au point un mécanisme de signalisation qui établirait des LSP après une panne.

Une autre amélioration pouvant donner suite à des travaux de recherche serait d'implémenter un mécanisme qui permet la mise à jour dynamique des chemins alternés suite à un changement de topologie.

Comme troisième piste de recherche, on peut penser à étendre cet algorithme à d'autres types de réseaux 3G ou même les réseaux optiques.

BIBLIOGRAPHIE

A. Autenrieth, A. Kirstädter, "Engineering End-to-End IP Resilience Using Resilience-Differentiated QoS", *IEEE Communications Magazine*, Vol. 40, No. 1, Jan 2002, pp. 50-57.

A. Autenrieth, A. Kirstädter, "RD-QoS - The Integrated Provisioning of Resilience and QoS in MPLS-Based Networks", *IEEE International Conference on Communications (ICC 2002)*, New York, USA, April 28 - May 02, 2002, pp. 1174-1178.

A. Autenrieth, A. Kirstädter "Fault Tolerance and Resilience Issues in IP based Networks", *Second International Workshop on the Design of Reliable Communication Networks*, München, April 10-12, 2000.

A. Kirstädter, A. Autenrieth, *An Extended QoS Architecture Supporting Differentiated Resilience Requirements of IP Services*, IETF Draft, draft-kirstaedter-extqosarch-00.txt, August 9, 2000.

A. Autenrieth, A. Kirstädter, "Provisioning of Differentiated IP Resilience and QoS-An Integrated Approach", *ITG Workshop "IP in Telekommunikationsnetzen"*, Bremen, January 26, 2001.

A. Autenrieth, A. Kirstädter, "Components of MPLS Recovery Supporting Differentiated Resilience Requirements", *7th EUNICE 2001*, September 3-5, 2001, Paris, France.

A. Autenrieth, A. Kirstädter, "Components of MPLS Recovery Supporting Differentiated Resilience Requirements", *IFIP Workshop on IP and ATM Traffic Management, WATM 2001,* September 3-5, 2001, Paris, France.

A. Farrel, B. Miller, *Surviving Failures in MPLS Networks*, Feb 2001, Data Connection Limited, Enfield, UK.

D. Awduche, L. Berger, T.Li, V.Srinivasan, G.Swallow, *RSVP-TE: Extension to RSVP for LSP tunnels*, RFC3029, Dec 2001.

R. Braden, L. Zhang, S. Berson, S. Herzog S. Jamin, *Resource Reservation protocol (RSVP) -- Version 1 Functional specification*, RFC2205, Sept 1997.

C. Hang, V. Sharma, S. Makam, K. Owens, *A Path Protection/Restoration Mechanism for MPLS Networks*, (work in progress) Internet Draft draft-chang-mpls-path-protection, Jul 2000.

D. Haskin, R. Krishnan, *A Method for Setting an Alternative Label Switched Paths to Handle Fast Reroute*, (work in progress) Internet Draft draft-haskin-mpls-fast-reroute, Nov 2000.

S. Kini, M. Kodialam, T.V. Lakshman, C. Villamizar, *Shared backup Label Switched Path restoration*, (work in progress) Internet Draft draft-kini-restoration-shared-backup, Oct 2000.

R. Krishnan, D. Haskin, *Extension to RSVP to Handle Establishment of Alternate Label-Switched-Paths for Fast Reroute*, (work in progress), Internet Draft draft-krishnan-mpls-reroute-resvpext-00.txt, June 1999.

K. H. Lee, Y. H. Choi, J. Y. Lee, S. B. Lee, "QoS restoration using a disjoint path group in ATM networks", *IM 1999 - IFIP/IEEE International Symposium on Integrated Network Management*, no. 1, May 1999 pp. 669-682.

K. Nichols, S. Blake, F. Baker, and D. Black, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*, RFC 2474, December 1998.

E.C. Ortega, *MPLS dynamic Multilevel protection*, Thèse de doctorat (PhD.), département d'informatique, d'automatique et d'électronique, Université de Girona, Juil 2001.

P. Ping, D. Gan, G. Swallow, J-P. Vasseur, D. Cooper, A. Atlas, M. Jork, *Fast Reroute Extension to RSVP-TE for LSP Tunnels*, (work in progress) Internet Draft draft-ietf-mpls-rsvp-lsp-fastreroute-00.txt, Jan 2002.

P. Pan, *Scalable Ressource Reservation Signaling in the Internet*, Thèse de Doctorat (PhD), Graduate School of Arts and Sciences, Columbia University, 2002.

V. Sharma, F. Hellstrand, *Framework for MPLS-based Recovery*, (work in progress), Internet Draft draft-ietf-mpls-recovery-frmwork-05.txt, May 2002.

P. Veitch, D. Johnson, "ATM network resilience", *IEEE Network*, no. 5, September/October 1997 pp. 26-33.

C. Vijayanand, *Fast Reroute Extensions to CRLDP*, (work in progress) Internet Draft draft-vijay-mpls-crldp-fastreroute-00.txt, Avril 2002